CLI REFERENCE

FortiMail™ Secure Messaging Platform Version 3.0 MR4

Note: The History sections in the command entries are intended to record changes in FortiMail 3.0 CLI commands with each release of the product. Although these sections show all commands as new for version 3.0, many of the commands existed in previous versions of FortiMail firmware.

FORTINET™

www.fortinet.com

FortiMail™ Secure Messaging Platform CLI Reference
Version 3.0 MR4
14 August 2008
06-30004-0420-20080814

Trademarks

Contents

Introduction

This chapter introduces you to the FortiMail™ Secure Messaging Platform and the following topics:

- About the FortiMail Secure Messaging Platform
- About this document
- FortiMail documentation
- Customer service and technical support

About the FortiMail Secure Messaging Platform

Each FortiMail unit is 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. The FortiMail unit has reliable and high performance features for detecting and blocking spam messages and malicious attachments. Built on Fortinet's FortiOS™, the FortiMail antivirus technology extends full content inspection capabilities to detect the most advanced email threats.

About this document

This document describes how to use the Fortinet Command Line Interface (CLI). The following chapters appear in this document:

- Using the CLI describes how to connect to and use the Fortinet command-line interface (CLI).
- execute is an alphabetically-ordered reference to the `execute` commands. These commands perform immediate actions on the FortiMail unit, such as configuration backup or unit reset.
- get is an alphabetically-ordered reference to the `get` commands. These commands display information about FortiMail unit configuration and status.
- set is an alphabetically-ordered reference to the `set` commands. These commands configure all aspects of FortiMail unit operation.
- unset is an alphabetically-ordered reference to the `unset` commands. These commands remove configurations such as alert email settings, LDAP profiles, logging and email server settings.

Note: Diagnose commands are also available from the FortiMail CLI. These commands are used to display system information and for debugging. Diagnose commands are intended for advanced users only, and they are not covered in this document. Contact Fortinet technical support before using these commands.

Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.
- Notes and Cautions are used to provide important information:

Note: Highlights useful additional information.

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

Typographic conventions

Fortinet documentation uses the following typographical conventions:

Convention	Example
Keyboard input	In the Gateway Name field, type a name for the remote VPN peer or client (for example, `Central_Office_1`).
CLI command syntax	`execute restore config <filename_str>`
Document names	*FortiMail Administration Guide*
File content	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4>`
Menu commands	Go to **Anti-Spam > Greylist > Exempt** and select Create New.
Program output	`Welcome!`
Variables	• `<xxx_str>` indicates an ASCII string variable keyword. • `<xxx_integer>` indicates an integer variable keyword. • `<xxx_ipv4>` indicates an IP address variable keyword. • vertical bar and braces `{|}` separate mutually exclusive required keywords For example: `set system opmode {gateway	transparent	server}` This example indicates you can enter `set system opmode gateway` or `set system opmode transparent` or `set system opmode server`

FortiMail documentation

Information about the FortiMail unit is available from the following guides:

- *FortiMail QuickStart Guides*

  Provides basic information about connecting and installing a FortiMail unit. A separate guide is available for each FortiMail model.
- *FortiMail Administration Guide*

  Introduces the product and describes how to configure and manage a FortiMail unit, including how to create profiles and policies, configure antispam and antivirus filters, create user accounts, configure email archiving, and set up logging and reporting.
- *FortiMail CLI Reference*

  Describes how to use the FortiMail CLI and contains a reference of all FortiMail CLI commands.
- *FortiMail Log Message Reference*

  Available exclusively from the Fortinet Knowledge Center, the FortiMail Log Message Reference describes the structure of FortiMail log messages and provides information about the log messages that are generated by FortiMail units.
- *FortiMail Installation Guide*

  Describes how to set up the FortiMail unit in transparent, gateway, or server mode.
- *FortiMail online help*

  Provides a searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiMail Webmail online help*

  Describes how to use the FortiMail web-based email client, including how to send and receive email, how to add, import, and export addresses, how to configure message display preferences, and how to manage quarantined email.
- *FortiMail User Guides*

  Provides information that the FortiMail end users need to know in order to take advantage of the services provided by the FortiMail unit. These guides are included as chapters in the *FortiMail Administration Guide*, allowing the administrator to provide information on only the enabled features.

Fortinet Tools and Documentation CD

All Fortinet documentation is available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation visit the Fortinet Technical Documentation web site at http://docs.forticare.com.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Center at http://kc.forticare.com.

Comments on Fortinet technical documentation

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

Customer service and technical support

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

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.

What’s new

The table below lists commands which have changed since the previous release, 3.0 MR3.

Command	Change
`execute partitionlogdisk`	New command. Sets the size of the hard disk partition to use as the log disk. Remaining hard disk space is used as the mail disk.
`set as bounceverify`	New command. Configures verification of delivery status notification (DSN) email.
`set as mms_reputation`	New command. Sets the window of time during which detection of multimedia message service (MMS) spam will affect the sender reputation of the end user ID (MSISDN).
`set as profile modify rewrite_rcpt`	New command. Configure rewriting of the recipient email address located in the envelope if the email message is detected as spam.
`set ip_profile headermanipulation`	New command. Removes specified message headers.
`set ip_profile mms_reputation`	New command. Enables or disables detection of spam based upon the sender reputation of the end user ID (MSISDN) for multimedia message service (MMS) email messages, and configures its detection threshold and duration.
`set ip_profile sendervalidation bypassbounceverify`	New keyword. Enables or disables bypass of verification of delivery status notification (DSN) email.
`set ip_profile_setting rate_control`	New command. Selects whether to rate control email messages by either the number of email messages or the number of SMTP connections.
`set mailserver access ... authenticated`	New keyword. Selects whether to apply the access control rule to only authenticated SMTP sessions, or regardless of authentication status.
`set mailserver access ... tlsprofile`	New keyword. Selects the name of a transport layer security (TLS) profile to apply to SMTP sessions governed by this access control rule.
`set mailserver smtp ldap_domain_check`	New command. Enables or disables use of an LDAP query to verify the existence of a domain and to automatically associate it with a protected domain.
`set mailserver smtpauth smtp`	New keyword. Enables or disables SMTP authentication.
`set mailserver smtpauth smtpovertls`	New keyword. Enables or disables transport layer security (TLS) authentication for SMTP.
`set mailserver smtpauth smtps`	New keyword. Enables or disables SMTPS authentication.
`set policy modify add_association`	New command. Configures domain associations, which associate a domain name with the settings for an existing protected domain.

Command	Change
`set system fortimanager`	New command. Configures remote administration by and automatic configuration backups to a FortiManager system.
`set user pki`	New command. Configures public key infrastructure (PKI) authentication for email users and FortiMail administrators.

Using the CLI

This section describes how to connect to and use the FortiMail command line interface (CLI). You can use CLI commands to view all FortiMail system information and to change all system configuration settings.

This section contains the following topics:

- CLI command syntax
- Connecting to the CLI
- CLI command branches

CLI command syntax

This guide uses the following conventions to describe command syntax.

- Angle brackets `< >` to indicate variables.

  For example:

  ```
  set console page <length_int>
  ```

  You enter:

  ```
  set console page 40
  ```

  The various types of variables include:

  `<xxx_str>` indicates an ASCII string.

  `<xxx_int>` indicates an integer string that is a decimal number.

  `<xxx_ipv4>` indicates a dotted decimal IPv4 address.

  `<xxx_v4mask>` indicates a dotted decimal IPv4 netmask.

  `<xxx_ipv4mask>` indicates a dotted decimal IPv4 address followed by a dotted decimal IPv4 netmask (e.g. 192.168.1.99 255.255.255.0)

  `<xxx_ipv4/mask>` indicates a dotted decimal IPv4 address followed by a CIDR notation IPv4 netmask (e.g. 192.168.1.99/24)

  `<xxx_ipv6>` indicates an IPv6 address.

  `<xxx_v6mask>` indicates an IPv6 netmask.

  `<xxx_ipv6mask>` indicates an IPv6 address followed by an IPv6 netmask.

- Vertical bar and braces `{|}` separate alternative, mutually exclusive required keywords.

  For example:

  ```
  set system opmode {gateway | server | transparent}
  ```

  You can enter `set system opmode gateway` or `set system opmode server` or `set system opmode transparent`.

- Square brackets `[ ]` to indicate that a keyword or variable is optional.

  For example:

```
set policy <fqdn> modify fallbackhost <host_ipv4>
   [fallbackport <port>]
```

The fallback host address is required, and a fallback port is optional

- A space to separate options that can be entered in any combination and must be separated by spaces.

  For example:

  ```
  set allowaccess {ping https ssh snmp http telnet}
  ```

  You can enter any of the following:

  ```
  set allowaccess ping
  ```

  ```
  set allowaccess ping https ssh
  ```

  ```
  set allowaccess https ping ssh
  ```

  ```
  set allowaccess snmp
  ```

  In most cases to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.

Connecting to the CLI

You can use a direct console connection, SSH, or Telnet to connect to the FortiMail unit CLI.

Connecting to the FortiMail unit console

To connect to the FortiMail console, you require:

- A computer with an available com port.
- A null modem cable to connect the FortiMail console port.
- Terminal emulation software such as HyperTerminal for Windows.

Note: The following procedure describes how to connect to the FortiMail CLI using Windows HyperTerminal software. You can use any terminal emulation program.

To connect to the FortiMail unit console

1. Connect the FortiMail console port to the available communications port on your computer.
2. Make sure the FortiMail unit is powered on.
3. Start HyperTerminal, enter a name for the connection, and select OK.
4. Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the FortiMail console port.
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 FortiMail CLI.

8 A prompt appears:

```
FortiMail-400 login:
```

9 Type a valid administrator name and press Enter.

10 Type the password for this administrator and press Enter.

The following prompt appears:

```
Welcome!
```

You have connected to the FortiLog CLI, and you can enter CLI commands.

Setting administrative access for SSH or Telnet

To configure the FortiMail unit to accept SSH or Telnet connections, you must set administrative access to SSH or Telnet for the FortiMail interface to which your management computer connects. To use the web-based manager to configure FortiMail interfaces for SSH or Telnet access, see “Interface settings” in the “Configuring FortiMail system settings” chapter of the *FortiMail Administration Guide*.

To use the CLI to configure SSH or Telnet access

1 Connect and log into the CLI using the FortiMail console port and your terminal emulation software.

2 Use the following command to configure an interface to accept SSH connections:

```
set system interface <interface_name> config allowaccess ssh
end
```

3 Use the following command to configure an interface to accept Telnet connections:

```
set system interface <interface_name> config allowaccess
telnet
```

4 To confirm that you have configured SSH or Telnet access correctly, enter the following command to view the access settings for the interface:

```
get system interface
```

The CLI displays the settings, including the management access settings, for the configured interfaces.

Connecting to the FortiMail CLI using SSH

Secure Shell (SSH) provides strong secure authentication and secure communications to the FortiMail CLI from your internal network or the internet. Once the FortiMail unit is configured to accept SSH connections, you can run an SSH client on your management computer and use this client to connect to the FortiMail CLI.

Note: The FortiMail unit supports the following encryption algorithms for SSH access: 3DES and Blowfish.

To connect to the CLI using SSH

1. Install and start an SSH client.
2. Connect to the FortiMail interface that is configured for SSH connections.
3. Type a valid administrator name and press Enter.
4. Type the password for this administrator and press Enter.

   The FortiMail model name followed by a # is Displayed.

   You have connected to the FortiMail CLI, and you can enter CLI commands.

Connecting to the FortiMail CLI using Telnet

You can use Telnet to connect to the FortiMail CLI from your internal network or the Internet. Once the FortiMail unit is configured to accept Telnet connections, you can run a Telnet client on your management computer and use this client to connect to the FortiLog CLI.

⚠ **Caution:** Telnet is not a secure access method. SSH should be used to access the FortiLog CLI from the internet or any other unprotected network.

To connect to the CLI using Telnet

1. Install and start a Telnet client.
2. Connect to the FortiMail interface that is configured for Telnet connections.
3. Type a valid administrator name and press Enter.
4. Type the password for this administrator and press Enter.

   You have connected to the FortiMail CLI, and you can enter CLI commands.

CLI command branches

The FortiGate command-line interface consists of four command branches:

- Use `execute` to run static commands on the FortiMail unit. Examples include resetting the device, formatting the hard drive, and pinging other devices from the FortiMail unit’s network interfaces.

  For a complete `execute` command list, see “execute” on page 25.
- Use `get` to display system status information. The `get` command can be used to display the current value of items configured with the `set` command.

  For a complete `get` command list, see “get” on page 49.
- Use `set` to configure the FortiMail unit. All of the configuration allowed in the GUI can also be accomplished using the `set` command. Some extra options not available in the GUI are also available with the `set` command.

  For a complete `set` command list, see “set” on page 93.
- Use `unset` to return settings to their default values.

  For a complete `unset` command list, see “unset” on page 353.

execute

Use `execute` commands to perform maintenance operations on your FortiMail unit or to perform network test operations such as ping or traceroute.

This chapter describes the following execute commands:

backup config
checklogdisk
checkmaildisk
clearqueue
factoryreset
formatlogdisk
formatmaildisk
formatmaildisk_backup
maintain
nslookup
partitionlogdisk
ping
ping-option
reboot
reload
restore
shutdown
smtptest
telnettest
traceroute
update config
updatecenter updatenow

backup config

Use this command to back up system settings to a TFTP server.

Syntax

```
execute backup config <name_str> <server_ipv4>
```

`<name_str>` is the filename for the backup on the TFTP server

`<server_ipv4>` is the IP address of the TFTP server

History

FortiMail v3.0	New.

Related topics

- execute restore

checklogdisk

When recommended by Customer Support, use this command to find and correct errors on the log disk. Logging is suspended while this command is running.

Syntax

```
execute checklogdisk
```

History

FortiMail v3.0	New.

Related topics

- execute checkmaildisk

checkmaildisk

When recommended by Customer Support, use this command to find and correct errors on the mail disk. Actions are reported at the command prompt. If the check can't fix something automatically, it presents a list of options for the admin to select from.

Mail functions are suspended while this command is running.

Syntax

```
execute checkmaildisk
```

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Renamed from `checkspooldisk`.

Related topics

- execute checklogdisk

clearqueue

Select to remove all messages from the deferred queue.

Syntax

```
execute clearqueue
```

History

FortiMail v3.0 MR3 New.

Related topics

- execute checklogdisk

factoryreset

Use this command to restore the factory default settings.

This will delete your configuration.

Syntax

```
execute factoryreset
```

History

FortiMail v3.0	New.

formatlogdisk

Use this command to reformat the local log hard disk to enhance performance.

This will delete the logs on the log disk.

Syntax

```
execute formatlogdisk
```

History

FortiMail v3.0	New.

Related topics

- execute formatmaildisk
- execute formatmaildisk_backup

formatmaildisk

Use this command to reformat the local email disk to enhance performance after you have backed up the mail database to the log disk with `execute formatmaildisk_backup`.

This will delete your mail database.

Syntax

```
execute formatmaildisk
```

History

FortiMail v3.0	New.

Related topics

- execute formatmaildisk_backup

formatmaildisk_backup

Use this command to back up the mail database to the log disk, and then format the local mail disk. This will enhance performance on the mail disk.

Syntax

```
execute formatmaildisk_backup
```

History

FortiMail v3.0	New.

Related topics

- execute formatmaildisk

maintain

Use this command to perform maintenance on mail queues by deleting out-of-date messages.

Syntax

```
  execute maintain mailqueue clear age <age>[<unit>]
```

`<age>` messages this age or older will be cleared, and can be from 1 hour to 10 years.

`<unit>` can be one of h, d, m, or y for hours, days, months, or years respectively.

The default is 24h.

Example

This example will clear messages that are 23 days old and older.

```
execute maintain mailqueue clear age 23d
```

History

FortiMail v3.0 MR3	New.

Related topics

- execute clearqueue

nslookup

Use this command to perform a name server lookup on the specified host or MX record.

Syntax

```
execute nslookup {host | mx} <name_server>
```

`<name_server>` can be an IP address or a fully qualified domain name.

History

FortiMail v3.0	New.

Related topics

- execute ping
- execute traceroute

partitionlogdisk

Use this command to adjust the ratio of disk space allocated to the logs and mail. By default, 75% of the disk space is allocated to mail and 25% to logs.

Syntax

```
execute partitionlogdisk <log_int>
```

`<log_int>` is the percentage of the total disk space allocated to log files. Specify any value between 10 and 90. The remainder is allocated to mail.

⚠ **Caution:** Executing this command formats the FortiMail disks. This operation deletes all mail and log data.

History

FortiMail v3.0 MR4 New.

Related topics

- execute formatlogdisk
- execute formatmaildisk
- execute formatmaildisk_backup

ping

Use this command to ping the specified host name or host IP address.

Syntax

```
execute ping {<host_name> | <host_ipv4>}
```

History

FortiMail v3.0	New.

Related topics

- execute ping-option

ping-option

Use this command to configure the ping function behavior settings.

Syntax

```
execute ping-option <option>
```

Option	Description	Default
`data-size <bytes>`	Enter datagram size in bytes.	`56`
`df-bit {yes | no}`	Enter `yes` to set the DF bit in the IP header to prevent the ICMP packet from being fragmented. Setting `df-bit` to no allows the ICMP packet to be fragmented.	`no`
`pattern <hex_pattern>`	Enter a pattern to fill the optional data buffer at the end of the ICMP packet, for example `00ffaabb`. The size of the buffer is specified using the `data_size` parameter. This allows you to send out packets of different sizes for testing the effect of packet size on the connection.	None
`repeat-count <integer>`	Enter the number of times to repeat the ping. The value must be greater than 0.	5
`source {auto | <ipv4>}`	Select the interface from which the ping is sent. Enter either `auto` or the interface IP address.	`auto`
`timeout <seconds>`	Enter the ping response timeout in seconds.	2
`tos <tos_value>`	Enter the IP type-of-service option value, one of: • `default` 0 • `lowcost` minimize cost • `lowdelay` minimize delay • `reliability` maximize reliability • `throughput` maximize throughput	`default`
`ttl <TTL_integer>`	Enter the time-to-live (TTL) value.	`64`
`validate-reply {yes | no}`	Enter `yes` to validate ping replies.	`no`
`view-settings`	View the current ping option settings.	`N/A`

History

FortiMail v3.0	New.

Related topics

- execute ping

reboot

Use this command to restart the FortiMail unit.

Syntax

```
execute reboot
```

History

FortiMail v3.0	New.

Related topics

- execute reload

reload

If you set your console to batch mode, use this command to flush the current configuration from system memory and reload the configuration from a saved configuration file.

Syntax

```
execute reload
```

History

FortiMail v3.0	New.

Related topics

- execute reboot

restore

Use this command to restore system configuration or firmware from a TFTP server.

Syntax

```
execute restore {config | image} <name_str> <server_ipv4>
```

Enter `config` to restore system settings or `image` to restore system firmware image.

`<name_str>` is the name of the configuration file on the TFTP server.
`<server_ipv4>` is the IP address of the TFTP server.

History

FortiMail v3.0	New.

Related topics

- execute backup config

shutdown

Use this command to prepare the FortiMail unit to be powered down. This command clears all buffers and writes all cached data to disk. Power off the FortiMail unit only after issuing this command to prevent possible data loss.

Syntax

```
execute shutdown
```

History

FortiMail v3.0	New.

Related topics

- execute reboot

smtptest

Use this command to test connectivity to an SMTP server.

Syntax

```
   execute smtptest <ipv4_addr[:port]> domain <domain_str>
```

<ipv4_addr> is the IP address of the SMTP server

[:port] is the optional port number to connect to the SMTP server.

<domain_str> is the name of the domain on the SMTP server to connect to.

Example

This example tests the connection to an SMTP server at 192.168.100.2 on port 25 to the example.com domain.

```
execute smtptest 192.168.100.2:25 domain example.com
```

History

FortiMail v3.0 MR3	New.

Related topics

- execute reboot

telnettest

Use this command to attempt a telnet connection to the specified host IP address.

Syntax

```
execute telnettest <host_ipv4[:port]>
```

If you do not specify a port number, port 23 is used.

History

FortiMail v3.0	New.

traceroute

Use this command to trace the route to the specified host IP address.

Syntax

```
execute traceroute <host_ipv4>
```

History

FortiMail v3.0	New.

Related topics

- execute maintain
- execute ping

update config

Use this command to request a configuration update from the FortiManager server.

Syntax

```
execute update config
```

History

FortiMail v3.0	New.

updatecenter updatenow

Use this command to manually initiate a virus definition update.

Syntax

```
execute updatecenter updatenow
```

History

FortiMail v3.0	New.

get

alertemail configuration

Use this command to view the alert email recipients. The command displays the SMTP server address, SMTP user name, SMTP authentication status, encrypted SMTP password, and the email addresses used to send the alert.

Syntax

```
get alertemail configuration
```

History

FortiMail v3.0	New.

Related topics

- get alertemail setting

alertemail setting

Use this command to view the alert email configuration. This command displays what is enabled or disabled for:

- virus incidents
- critical events
- disk full
- archiving failure
- HA events
- dictionary corruption
- system quarantine quota full

Syntax

```
get alertemail configuration
```

Example

```
FortiMail-400 # get alertemail setting
Alert email setting:
        alert email for antivirus:              disabled
        alert email for critical events:        disabled
        alert email for disk full:              enabled
        alert email for archiving failure:      enabled
        alert email for HA events:              disabled
        alert email for Dictionary corruption:  disabled
        alert email for system quarantine quota is full: disabled
        alert email for Defer queue:            enabled
```

History

FortiMail v3.0	New.

Related topics

- get alertemail configuration

antivirus

Use this command to display whether antivirus scanning is enabled. This is available only in server mode.

Syntax

```
get antivirus
```

Example

```
FEServer # get antivirus
global antivirus scanning is enabled
```

History

FortiMail v3.0	New.

as

Use this command to display information about your antispam configuration.

Syntax

```
get as <option>
```

Option	Description
`blacklistaction`	Display the action set for blacklisted items.
`control autorelease`	Display the spam auto release and auto delete account names.
`control bayesian`	Display the Bayesian training account names.
`greylist`	Display the greylist settings, including the TTL, greylist period, initial expiry period, capacity, and exempt address list.
`profile <profile_name>`	Display the settings of an antispam profile.
`spamreport`	Display the quarantine spam report settings.
`trusted antispam-mta`	Display the IP addresses on the antispam-MTA list.
`trusted mta`	Display the IP addresses on the MTA list.

Examples

```
FortiMail-400 # get as blacklistaction
blacklist action: reject

FortiMail-400 # get as control autorelease
autorelease account is release-ctrl
autodelete account is delete

FortiMail-400 # get as control bayesian
"is spam" account is is-spam
"is not spam" account is is-not-spam
"learn is spam" account is learn-is-spam
"learn is not spam" account is learn-is-not-spam
"training group" account is default-grp

FortiMail-400 # get as greylist

TTL: 10 (day)
Greylist period: 20 (minute)
Initial expiry period: 4 (hour)
Capacity: 40000

Greylist exempt:

FortiMail-400 # get as profile profile2
Antispam profiles
 id=3, name=profile2
  Heuristic filtering: enabled
    action: default
    lower level: -15.000000
    upper level: 5.000000
  Bayesian filtering: enabled
```

```
    action: default
    use personal database: disabled
    Accept training from users: disabled
    Use other techniques for auto training: disabled
  Deepheader filtering: disabled
    action: default
    check black ip: enabled
    headers analysis: enabled
  Dictionary filtering: disabled
    action: default
    dictionary profile: unknown(-1)
  FortiGuard-Antispam filtering: disabled
    action: default
    FortiGuard-Antispam checkip: disabled
  Dnsbl server lookup: disabled
    action: default
  Surbl server lookup: disabled
    action: default
  Banned word scanning: disabled
    action: default
  Whitelist word scanning: disabled
  Greylist message senders:  disabled
  Treat message with virus as spam:  disabled
    action: default
  Check forged IP in incoming emails:  disabled
    action: default
  Check image spam in incoming emails: disabled
    action: default
    Check image spam aggressively: disabled
  Scan conditions:
    maxsize: 0
    bypass_on_auth:      disabled
    attachment types:
       pdf: disabled
  Actions:
    discard reject
    subject tagging: disabled, tag=""
    header  tagging: disabled, tag=""
    quarantine is: enabled
      auto delete:  enabled, number of days=7
      auto release of quarantined emails by email: disabled
      auto release of quarantined emails by web: disabled
      add the sender of a released message to personal white list: 
  disabled
    allow users to automatically update personal White list from sent 
  emails:  disabled

FortiMail-400 # get as spamreport
time of day: 00:00
interval: these hours:
Web Release Hostname is empty
 Web Release through HTTPS is enabled
```

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Added `trusted antispam-mta` and `trusted mta` commands.

auth

Use this command to display authentication settings by protocol: IMAP, POP3, RADIUS, SMTP. This is available in transparent and gateway modes only.

Syntax

```
get auth {imap | pop3 | radius | smtp}
```

History

FortiMail v3.0	New.

av

Use this command to display the settings of an antivirus profile.

Syntax

```
get av <profile_name>
```

Example

```
FortiMail-400 # get av avprofile1
Antivirus profiles
 id=2, name=avprofile1
  AV Scanner:  enabled
  AV actions:
  Heuristic scanning:  disabled
  Heuristic actions:
```

History

FortiMail v3.0	New.

config

Use this command to display the current FortiMail unit configuration.

Syntax

```
get config [<search_string>]
```

`<search_string>` is an optional search string. If the string contains spaces, enclose it in single quotation marks (' ').

If you specify a search string, the command displays only the lines in the configuration file that contain that string. Otherwise, the command lists the entire configuration.

History

FortiMail v3.0	New.

console

Use this command to display console settings: the number of lines per page, the mode of operation, and the baud rate of the command line console.

Syntax

```
get console
```

Example

```
FortiMail-400 # get console
Page number: 24
Console mode: Line
Console baudrate: default
```

History

FortiMail v3.0	New.

fshd status

Use this command to display the FortiGuard settings on the FortiMail unit.

Syntax

```
get fshd status
```

Example

```
FortiMail-400 # get fshd status
Fortishield service status: enabled
Fortishield service cache status: enabled
Fortishield service cache ttl: 600
Fortishield service hostname antispam.fortigate.com
```

History

FortiMail v3.0	New.

ip_policy

Use this command to list information about IP policies.

Syntax

```
get ip_policy [<policy_number>]
```

If you do not specify a policy number, the command provides a list of the IP policies, by name and number. If you specify a policy number, the command lists detailed information about that policy.

Example

```
FortiMail-400 # get ip_policy 0
smtpin configuration 0
        matches: from 0.0.0.0/0, to 0.0.0.0/0
         action: SCAN
     ip profile: 'session_strict'
      exclusive: this profile can be overriden by a recipient profile
           SMTP: is disabled, and difference are NOT allowed
```

History

FortiMail v3.0	New.

Related topics

- get ip_profile

ip_pool

Use this command to list information about IP pool policies.

Syntax

```
get ip_pool {<name_str>}
```

If you do not specify a policy name, the command returns a list of the IP pool policies, by name and ID number. If you specify a policy name, the command lists the IP ranges defined in the policy.

History

FortiMail v3.0 MR3 New.

Related topics

- get ip_profile
- set ip_pool
- set ip_pool add_entry

ip_profile

Use this command to list information about IP profiles.

Syntax

```
get ip_profile [<profile_name>]
```

If you do not specify a profile name, the command provides a list of the IP profiles.

If you specify a profile name, the command lists detailed information about that IP profile.

Example

```
FortiMail-400 # get ip_profile session_loose
smtpin configuration for "session_loose"
    connection: rate limiting per IP is disabled
                this box will NOT be hidden from the server
                connection limiting per IP is disabled
                total connection limiting is disabled
                preventing connections to blacklisted SMTP is disabled
                idle timeout is disabled
       session: checking HELO/EHLO chars is disabled
                HELO/EHLO rewrite is disabled
                disallowing encrypted links is disabled
                allow pipelining NO
                strict synax checking is disabled
                splice is disabled
                ACK EOM before anti-spam is disabled
                Send DSN to sender when spam detected is disabled
           (for unauthorised links)
                checking sender domain is disabled
                checking recipient domain is disabled
                reject empty domains is disabled
                open relay checking is disabled
                RCPT/HELO/MAIL domain check is disabled
        limits: max number of recipients per email is 500
                no helo/ehlo per session
                no email per session
                max supported message size is 10485760
                max supported header size is 32768
                no NOOP restrictions
                no RSET restrictions
        errors: no "free" errors
                there is no initial error delay
                subsequent errors use the initial delay
                the link will not disconnect because of errors
         lists: sender white list checking is disabled
                sender black list checking is disabled
                recipient white list checking is disabled
                recipient black list checking is disabled
 sender reputation: sender reputation  list checking is disabled
```

History

FortiMail v3.0	New.

Related topics

- get ip_policy

ldap_profile

Use this command to display all the settings of the specified LDAP profile.

Syntax

```
get ldap_profile profile <name_str>
```

`<name_str>` is the LDAP profile name.

To see a list of LDAP profiles, enter `get ldap_profile profile ?`.

History

FortiMail v3.0	New.

limits

Use this command to display all the settings of the limits command.

Syntax

```
get limits
```

<name_str> is the LDAP profile name.

To see a list of LDAP profiles, enter `get ldap_profile profile ?`.

Example

If you enter the `gets limits` command on a FortiMail-400 unit, the output will be similar to this:

```
FortiMail-400 # get limits

  domain level limits
    domains with 2 tier admin   25    (25   ) [500]
    admins per domain           5     (5    ) [5]
    policies per domain         40    (40   ) [40]
    profiles per domain         5     (5    ) [5]

  system level limits
    admin count                 20    (20   ) [20]
    total domains               500   (500  ) [500]
    total user groups           100   (100  ) [100]
    members per user group      50    (50   ) [50]
    profile count               50    (50   ) [50]
    ip policy count             40    (40   ) [40]
    outgoing policy count       500   (500  ) [500]
    as profile count           *175   (*175 ) [175]
    av profile count           *175   (*175 ) [175]
    content profile count      *175   (*175 ) [175]
    ip profile count           *175   (*175 ) [175]
    all shared memory size       13954552 (13954552) [268435456] bytes
    dynamic shared memory size   10273300 (10273300) [268435456] bytes

  (numbers in brackets indicates value to use on next reboot)

  [numbers in square brackets indicates maximum allowable values]

  (numbers preceeded by * are automatically calculated)
```

History

FortiMail v3.0 MR3 New.

Related topics

- set limits domain-level
- set limits system-level general
- set limits system-level groups
- set limits system-level mail-users
- set limits system-level other-profiles
- set limits system-level policies

log elog

FortiMail v3.0 New.

Use this command to display the event log messages that have been saved to local hard disk or remote syslog server.

Syntax

```
get log elog
```

History

FortiMail v3.0	New.

Related topics

- set log policy destination event
- set log setting local
- set log setting syslog

log logsetting

Use this command to display:

- the log to locations and whether logging to that location is turned on or off.
- the log severity level for each log location
- log file size
- log time
- log option setting when disk is full

Syntax

```
get log logsetting
```

Example

```
FortiMail-400 # get log logsetting
Log to remote syslog server 1:  OFF :514 level: emergency facility: kern
  CSV:OFF
Log to remote syslog server 2:  OFF :514 level: emergency facility: kern
  CSV:OFF
Log to Console:                 OFF level: emergency
Log to Local Host:              ON level: information
        Log file size: 10 Megabytes
        Log time: 10 days
        When reaching log file size or log time:        Overwrite
```

History

FortiMail v3.0	New.

Related topics

- set log setting local
- set
- set log setting syslog

log msisdn

Use this command to find out if the MSISDN column is enabled.

Use the `set log msisdn` command to enable the MSISDN column to display in **Log & Report** > **Logging**.

Syntax

```
get log msisdn
```

History

FortiMail v3.0 MR3 New.

Related topics

- set log msisdn
- set log view fields

log policy

Use this command to display information about log policies by destination and log type.

Syntax

To view which types of logging are enabled for each destination:

```
get log policy
```

To view detailed information about which types of logging are enabled for a destination:

```
get log policy [destination {syslog [number
  <integer>] | local | console}]
```

To view detailed information about a particular type of logging enabled for a destination:

```
get log policy [destination {syslog number <integer> | local | console}
  {event | history | spam | virus}]
```

Example

```
FortiMail-400 # get log policy destination syslog number 1 event
syslog 1 event:
        status: enable
        configuration:    ON
        ha:               OFF
        login:            ON
        pop3:             ON
        smtp:             ON
        system:           ON
        updatefailed:     ON
        updatesucceeded:  OFF
        webmail:          ON
```

History

FortiMail v3.0	New.

Related topics

- set log policy destination event
- set log policy destination spam
- set log policy destination virus
- set log setting local
- set
- set log setting syslog

log query

Use this command to display all available log query reports, for example, Top_Remote_Virus_Domain_by_Hour_of_Day. The total number of query reports displays at the bottom of the list.

Syntax

```
get log query
```

History

FortiMail v3.0	New.

Related topics

- set log reportconfig qry

log reportconfig

Use this command to display the settings in a saved log report configuration. The two default reports that become available after setting up your FortiGate unit with the quick start wizard, are also available for this command.

Syntax

```
get log reportconfig <config_name_str> <predefined_report_yesterday>
  <predefined report_last_week>
```

`<config_name_str>` is the log report configuration name. For a list of all saved log report configurations, enter “?” as the name.

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	The keywords, `predefined_report_yesterday` and `predefined_report_last_week` were added.

Related topics

- set log reportconfig direction
- set log reportconfig domain
- set log reportconfig mailto
- set log reportconfig period
- set log reportconfig qry
- set log reportconfig schedule hour

log view

Use this command to display what columns display in **Log & Report** > **Logging** for event, history, spam, and virus logs.

Use the `set log view` command to set the fields to display and the log severity level.

Syntax

```
get log view {event | history | spam | virus}
```

History

FortiMail v3.0	New.

Related topics

- set log view fields
- set log view loglevel
- set log policy destination event
- set log policy destination spam
- set log policy destination virus
- set log policy destination history

mailserver

Use this command to display the FortiMail email system settings.

Syntax

```
get mailserver
```

Example

```
FortiMail-400 # get mailserver

dead mail kept:           1 days
mail storage:             local disk
Centralized Quarantine:   Disabled
maximum message size:     10 MB
POP3 server port:         110
SMTP authentication:      enabled
SMTP over SSL:            disabled
SMTP server port:         25
SMTPS server port:        465


Relay server disabled
```

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Updated output.

Related topics

- get mailserver access
- get mailserver archive
- get mailserver localdomains
- get mailserver smtp
- get mailserver systemquarantine

mailserver access

Use this command to display the permissions for sending and receiving email for each domain.

Syntax

```
get mailserver access
```

History

FortiMail v3.0	New.

Related topics

- get mailserver
- get mailserver archive
- get mailserver localdomains
- get mailserver smtp
- get mailserver systemquarantine

mailserver archive

Use this command to display information about email archiving.

Syntax

To view email archiving account settings:

```
get mailserver archive
```

For other information:

```
get mailserver archive {exemptlist | local | policy | remote}
```

Option	Description
`exemptlist`	Display the archiving policy exceptions that exempt certain email from being archived.
`local`	Display the disk quota for archiving to the local hard disk.
`policy`	Display the email archiving policies.
`remote`	Display the settings for remote archiving via FTP or SFTP.

Example

This example shows the output without options.

```
FortiMail-400 # get mailserver archive
email archiving destination:  local
email archiving account:      archive
email archiving forward:
email archiving status:       disabled
Mailbox rotate size:          100 Megabytes
Mailbox rotate time:          7 Days
When reaching disk quota:     Overwrite
```

History

FortiMail v3.0	New.

Related topics

- get mailserver
- get mailserver access
- get mailserver localdomains
- get mailserver smtp
- get mailserver systemquarantine

mailserver localdomains

Use this command to display information about the domains added to the FortiMail unit. This is available in server mode only.

Syntax

```
get mailserver localdomain
```

History

FortiMail v3.0	New.

Related topics

- get mailserver
- get mailserver access
- get mailserver archive
- get mailserver smtp
- get mailserver systemquarantine

mailserver smtp

Use this command to display settings for SMTP email.

Syntax

```
get mailserver smtp <setting>
```

Variables	Description	
`<setting>`	Enter the setting, one of:	
	`deferbigmsg`	Display the times to start and stop delivering messages deferred because of their size.
	`dsn_displayname`	Display the sender name used in DSN messages.
	`dsn_sender`	Display the sender address used in DSN messages.
	`queue`	Display the parameter settings for time outs and retries for undelivered mail in queues.

History

FortiMail v3.0	New.
FortiMail v3.0 MR2	Added `queue` keyword.

Related topics

- get mailserver
- get mailserver access
- get mailserver archive
- get mailserver localdomains
- get mailserver systemquarantine

mailserver systemquarantine

Use this command to display the system quarantine settings. The system quarantine is used for mail matching content profiles.

Syntax

```
get mailserver systemquarantine
```

Example

```
FortiMail-400 # get mailserver systemquarantine
system(content) quarantine account:     systemquarantine
system(content) quarantine forward:
system(content) quarantine disk quota:  1 GB
system(content) quarantine rotate size: 100 Megabytes
system(content) quarantine rotate time: 7 Days
When reaching disk quota:               Overwrite
```

History

FortiMail v3.0	New.

Related topics

- get mailserver
- get mailserver access
- get mailserver archive
- get mailserver localdomains
- get mailserver smtp

misc profile

Use this command to display the misc profile settings. Available in server mode only.

Syntax

```
get misc [<profile_name>]
```

If you do not specify a profile name, the command displays information for all misc profiles.

Example

```
FEServer # get misc profile misc_def
Misc profiles
 id=0, name=misc_def
  User Account Status:  enabled
  Webmail Access:  enabled
  disk quota:  100
```

History

FortiMail v3.0	New.

out_content

Use this command to display outgoing content profile settings.

Syntax

```
get out_content [<name_str>]
```

`<name_str>` is the name of an outgoing content profile.

If you do not specify a profile, the command shows the settings of all outgoing content profiles.

History

FortiMail v3.0	New.

Related topics

- get out_policy
- get out_profile

out_policy

Use this command to display outgoing recipient-based policy settings.

Syntax

```
get out_policy [<name_str>]
```

`<name_str>` is the name of an outgoing policy.

If you do not specify a policy, the command shows the settings of all outgoing policies.

History

FortiMail v3.0	New.

Related topics

- get out_content
- get out_profile

out_profile

Use this command to display outgoing antispam profile settings.

Syntax

```
get out_profile [<name_str>]
```

`<name_str>` is the name of an outgoing antispam profile.

If you do not specify a profile, the command shows the settings of all outgoing profiles.

History

FortiMail v3.0	New.

Related topics

- get out_content
- get out_policy

policy

Use this command to display incoming recipient-based policies for domains. This is available only in transparent and gateway modes.

Syntax

```
get policy [<fqdn>]
```

`<fqdn>` is the domain's fully-qualified domain name.

If you do not specify a domain, the command shows the policies of all domains.

History

FortiMail v3.0	New.

Related topics

- get out_policy

spam deepheader

Use this command to display the deep header scan settings.

Syntax

```
get spam deepheader
```

Example

```
FortiMail-400 # get spam deepheader
  Deep header scanner setting:
  Confidence degree : 95.000000
  IP list of trusted server:
  Trusted IP list :
```

History

FortiMail v3.0 MR1 New.

Related topics

- set as profile modify deepheader
- set out_profile profile modify deepheader

spam heuristic rules

Use this command to display the total number of heuristic antispam rules. The number of rules can change as the FortiGuard service updates the heuristic rule set.

Syntax

```
get spam heuristic rules
```

Example

```
FortiMail-400 # get spam heuristic rules
The total amount of rules is: 88
```

History

FortiMail v3.0	New.
FortiMail v3.0 MR1	Removed keywords `desc`, `disabled`, `index`, `modified`, `name`, `status`, because the heuristic rules are now maintained by the FortiGuard service.

Related topics

- set as profile modify heuristic
- set out_profile profile modify heuristic

spam retrieval policy

Use this command to display spam retrieval policy information for a domain. This is available in transparent and gateway modes only.

Syntax

```
get spam retrieval policy <fqdn_str>
```

`<fqdn_str>` is the fully qualified domain name.

History

FortiMail v3.0	New.

system

Use this command to display system information.

Syntax

```
get system <item>
```

<item>	Description
`admin`	Display the current list of FortiMail administrator accounts including the user name, the IP address and netmask from which this account can manage the FortiMail unit, and the account read and write permissions.
`appearance`	Display the product name and bottom logo URL for the system logon page.
`autoupdate`	Display the antivirus engine version, antivirus definition version, update configuration, and update status.
`ddns`	Display the dynamic DNS information.
`disclaimer`	Display settings for header and body disclaimers for both incoming and outgoing email.
`dns`	Display the IP addresses of the primary and secondary DNS servers that the FortiMail unit uses for DNS lookups.
`ha`	Display HA status and configuration information for a FortiMail unit operating in active-passive or config only HA mode. If the FortiMail unit is operating in active-passive HA mode, the command displays the HA original and effective mode (also known as the HA configured and effective operating modes respectively), HA main and daemon configuration settings, and also lists peers in the HA group. If the FortiMail unit is operating in config only HA mode this command displays the HA mode (`cmaster` or `cslave`) and HA main and daemon configuration settings. If the FortiMail unit is operating in config only HA mode this command also displays the master configuration.
`hwraid`	Display the RAID settings.
`interface`	Display the configuration and status of all FortiMail unit network interfaces.
`kernel`	Display the kernel parameter configuration.
`localdomainname`	Display the name of the local domain.
`monitor`	Display the network interface monitoring configuration and status.
`objver`	Display the antivirus engine and virus definition versions, contract expiry date, and last update attempt result information.
`option`	Display system options, including system idle timeout, authentication timeout, and language for the web-based manager.
`performance`	Display the FortiMail unit system performance, including CPU usage, memory usage, and uptime.
`route table`	Display the FortiMail unit static routing table. For each route in the routing table, the command displays the route number, the destination IP address and netmask, and the gateways and interface for each static route.
`serialno`	Display the FortiMail unit serial number.
`snmp community`	Display the configuration and status of each defined SNMP community including community name, status, hosts, queries, traps, and events configured.
`snmp sysinfo`	Display the SNMP system information including the location, description and contact information for this FortiMail unit. This information is associated with the FortiMail unit's SNMP information when it is being managed.

<item>	**Description**
`snmp threshold`	Displays the SNMP threshold settings for available traps such as CPU usage, and memory usage.
`status`	Display system status information.
`time ntp`	Display the NTP configuration, including whether NTP is enabled, the NTP server IP address, and the NTP synchronization interval.
`time time`	Display the system date, time, time zone, and whether daylight saving time is enabled.
`usrgrp domain`	Display a list of the configured domain names.
`usrgrp domain [<name_str>]`	Display the user groups, including members of each user group, for the specified domain.

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Added `ddns`, and `localdomainname` keywords.

user

Use this command to display information about users.

Syntax

```
get user <item>
```

<item>	**Description**
`alias`	Display each user alias name and the included members.
`group`	Display each user group name and the included members. This is available only in server mode.
`ldap map`	This is available only in server mode.
`mail`	Display email accounts information, including user names and display names. This is available in server mode only.
`map`	Display a list of user mappings. This is available only in gateway and transparent modes.

History

FortiMail v3.0 New.

Related topics

- get userpolicy

userpolicy

Use this command to display the policy for a specified user. This is available in server mode only.

Syntax

```
get userpolicy <name_str>
```

`<name_str>` is the user name.

History

FortiMail v3.0	New.

Related topics

- get user

set

This chapter describes the following commands:

alertemail configuration mailto

alertemail deferq

alertemail setting option

antivirus

as blacklistaction

as control autorelease, as control bayesian

as greylist

as profile delete

as profile modify ...

as spamreport

as trusted

auth imap rename-to, auth imap server

auth pop3 rename-to, auth pop3 server

auth radius rename-to, auth radius server

auth smtp rename-to, auth smtp server

av delete

av modify ...

av rename-to

console

content delete, content modify ...

fshd

ip_policy ...

ip_pool ...

ip_profile ...

ldap_profile ...

limits ...

log msisdn

log policy destination ...

log reportconfig ...

log setting ...

log view fields, log view loglevel

mailserver access

mailserver archive ...

mailserver deadmail

mailserver portnumber

mailserver proxy smtp interface

mailserver proxy smtp unknown

mailserver relayserver

mailserver smtp ...

mailserver systemquarantine

misc profile delete

misc profile modify ...

misc profile rename-to

out_content delete

out_content modify ...

out_policy profile delete

out_policy modify

out_policy move-to, out_policy rename-to

out_profile profile delete

out_profile profile modify ...

out_profile profile rename-to

policy delete

policy modify ...

spam deepheader

spam retrieval policy

system ...

user

userpolicy delete

userpolicy modify

userpolicy move-to

userpolicy rename-to

alertemail configuration mailto

Use this command to set the email addresses of up to three alert email recipients.

Syntax

To set email recipients:

```
set alertemail configuration mailto <recipient1> [<recipient2>]
  [<recipient3>]
```

To remove all email recipients:

```
set alertemail configuration mailto none
```

Variables	Description	Default

`<recipient1>`
`<recipient2>`
`<recipient3>`
	Enter an email address in the form, name@emaildomain. You can add only three email addresses.	No default.

History

FortiMail v2.8	New.

Related topics

- set alertemail deferq
- set alertemail setting option

alertemail deferq

Use this command to configure the deferred email queue alert email conditions. You can set the number of deferred messages that trigger an alert email message, and how frequently the size of the deferred queue is monitored. This is effective only if `alertemail setting option deferq` is set.

Syntax

```
set alertemail deferq trigger <trigger_value> interval <interval_minutes>
```

Variables	Description	Default
`<trigger_value>`	Set the size that the deferred email queue must reach to cause an alert email to be sent. The range is 1 to 99999.	`10 000`
`<interval_minutes>`	Set the interval in minutes between checks of deferred queue size. This can be any number greater than zero.	`30`

History

FortiMail v2.8	New.

Related topics

- set alertemail configuration mailto
- set alertemail setting option

alertemail setting option

Use this command to set which alert email events are enabled. To disable all alert email events, use the none option.

Syntax

```
set alertemail setting option {<option_list> | none}
```

Variables	Description		Default
`<option_list>`	A space-delimited list of events that trigger alert email. Valid options are:		No default.
	`virusincidents`	Viruses detected.	
	`critical`	FortiMail unit detects a system error.	
	`diskfull`	The FortiMail unit hard disk is full.	
	`archivefailure`	Archiving to the remote host has failed.	
	`ha`	There is High Availability (HA) activity on the FortiMail unit.	
	`quotafull`	An account reached its disk quota.	
	`dictionary`	A dictionary is corrupt.	
	`systemquarantine`	System quarantine reached its quota.	
	`deferq`	The deferred mail queue exceeds the number of messages specified in `set alertemail deferq trigger`.	
	`none`	No events.	

Example

To enable alert email for full hard disk and account quota reached

```
set alertemail setting option diskfull quotafull
```

History

FortiMail v2.8	New.

Related topics

- set alertemail configuration mailto
- set alertemail deferq

antivirus

Use this command to enable or disable antivirus scanning. This command is available in server mode only.

Syntax

```
set antivirus {enable | disable}
```

History

FortiMail v3.0	New.

Related topics

- set ip_policy as
- set policy modify user
- set out_policy modify
- set userpolicy modify
- get antivirus

as blacklistaction

Use these commands to set the action to take when an email message arrives from a blacklisted email address, domain, or IP address. This setting affects mail matching all three levels of black lists: system, session, and user.

Syntax

```
set as blacklistaction {reject | discard | profile}
```

Keywords and Variables	Description	Default
`reject`	Reject the message and return an error to the computer attempting to deliver it.	`reject`
`discard`	Accept the message but discard it without notifying the sending system.	
`profile`	Use the setting in the anti-spam profile active for the blacklisted message.	

History

FortiMail v3.0	New.

Related topics

- set as profile modify whitelistword

as bounceverify

Use these commands to configure the bounce verification feature.

Spammers sometimes use the email addresses of others as the from address in their spam email messages. When the spam cannot be delivered, a delivery status notification message, or a bounce message, is returned to the sender, which in this case isn't the real sender. Because the invalid bounce message is from a valid mail server, it can be very difficult to detect as invalid.

You can combat this problem with bounce verification.

Syntax

```
set as bounceverify action {discard | reject | profile}
set as bounceverify autodeletepolicy {0 | 1 | 2 | 3 | 4}
set as bounceverify keys {activate | add | delete}
set as bounceverify status {enable | disable}
set as bounceverify tagexpiry <expiry_int>
```

Keywords and Variables	Description	Default
`action {discard	reject	profile}`	If a bounce message is invalid, this setting determines what the FortiMail unit will do with it. • **discard** will have the FortiMail unit accept the message and silently delete it. Neither the sender nor the recipient will be informed. • **reject** will have FortiMail unit reject the message. The system attempting delivery will receive an error. • **profile** will have the FortiMail unit use the action set in the applicable antispam profile.	
`autodeletepolicy {0	1	2	3	4}`	Inactive keys will be removed after being unused for the selected time period. • 0. Never automatically delete an unused key. • 1. Delete a key when it hasn't been used for 1 month. • 2. Delete a key when it hasn't been used for 3 months. • 3. Delete a key when it hasn't been used for 6 months. • 4. Delete a key when it hasn't been used for 12 months. The active key will not be automatically removed.	
`keys {activate	add	delete}`	Bounce verification keys can be activated, added, and deleted. • **activate** allows you to specify which key will be used to generate email message tags. Only one key can be active. • **add** allows you to create a new key by entering the key string. • **delete** allows you to delete an existing key by entering the key string.	
`status {enable	disable}`	Enable or disable bounce verification. Tag checking can be bypassed in each ip profile.	
`tagexpiry <expiry_int>`	Enter the number of days an email tag is valid. When this time elapses, the FortiMail unit will treated the tag as invalid.	

History

FortiMail v3.0 MR4 New.

Related topics

- set ip_profile sendervalidation

as control autorelease

Use these commands to set the control account names used to delete or release email messages from quarantine.

Syntax

```
set as control autorelease {delete | release} <control_account>
```

Keywords and Variables	Description	Default
`delete`	This keyword sets the email address ID used to delete quarantined messages.	`delete-ctrl`
`release`	This keyword sets the email address ID used to release quarantined messages.	`release-ctrl`
`<control_account>`	This is an email address ID. It is not a full email address, but only the portion before the @ symbol.	

The autorelease address IDs do not include a domain. The sender must use the domain appearing in their email address. This allows the autorelease address IDs to be valid for any domain configured on the FortiMail unit.

Example

To make the addresses more descriptive by setting the delete account ID to `quarantine_delete` and the release account to `quarantine_release`, enter these two commands:

```
set as control autorelease delete quarantine_delete
set as control autorelease release quarantine_release
```

A user with the email address user1@example.com would delete message from their quarantine by sending deletion requests to quarantine_delete@example.com. Similarly, this user would release quarantined email by sending release request messages to quarantine_release@example.com.

History

FortiMail v3.0	New.

Related topics

- set spam retrieval policy
- set as spamreport
- set as profile modify quarantine

as control bayesian

Use these commands to set the names for Bayesian control accounts.

Syntax

```
set as control bayesian is-spam <name_str>
set as control bayesian is-not-spam <name_str>
set as control bayesian learn-is-spam <name_str>
set as control bayesian learn-is-not-spam <name_str>
set as control bayesian training-group <sender_str>
```

Keywords and Variables	Description	Default
`is-spam`	FortiMail end users can send spam messages that were incorrectly treated as non-spam to this account to inform the Bayesian antispam check of its mistake.	`is-spam`
`is-not-spam`	FortiMail end users can send non-spam messages that were incorrectly treated as spam to this account to inform the Bayesian antispam check of its mistake.	`is-not-spam`
`learn-is-spam`	End users send known spam to this account to train the FortiMail unit. Based on the sender’s email address, the FortiMail unit uses the information received to train the sender’s Bayesian database.	`learn-is-spam`
`learn-is-not-spam`	End users send existing non-spam email to this account to train the FortiMail unit. Based on the sender’s email address, the FortiMail unit uses the information received to train the sender’s Bayesian database.	`learn-is-not-spam`
`training-group`	This account contains a system-wide spam database set up by the administrator. Using this account name as the “from” address, the administrator sends confirmed spam to the “learn-is-spam” user account and good email to the “learn-is -not -spam” user account to do group Bayesian training. If an individual user’s Bayesian database does not contain sufficient information for spam scanning, it will use the data received from the training group user account to scan spam.	`default-grp`
`<name_str>`	This is the name for this account. Users send messages to the email address composed of this name, followed by “@”, followed by the email domain.	
`<sender_str>`	This is the ‘from’ name used when sending mail to one of the other four accounts. Mail can be sent to correct incorrectly categorized mail, or to train the Bayesian database with new mail. Administrators send messages from the email address composed of this name, followed by “@”, followed by the email domain.	

Example

An administrator wants to change two of the Bayesian control account names. He knows his users will be better able to remember the addresses user to train the database with new messages if they include the word ‘train’:

The learn-is-spam command becomes train-is-spam and the learn-is-not-spam command becomes train-is-not-spam. To make these changes, enter these commands:

```
set as control bayesian learn-is-spam train-is-spam
set as control bayesian learn-is-not-spam train-is-not-spam
```

A user with the email address user1@example.com who received a spam message not marked as spam would send it to is-spam@example.com to inform the Bayesian database of its error. Similarly, a good message incorrectly marked as spam would be forwarded to is-not-spam@example.com. These two control address IDs are the defaults, and the domain is taken from the user's email address domain.

The two control address IDs the administrator modified are for training the Bayesian database with messages that have not been examined by the Bayesian filter. The user with the email address user1@example.com would submit spam messages to train-is-spam@example.com and good messages to train-is-not-spam@example.com.

To perform group training of the example.com group database or the global database (which ever is enabled) without similarly training his own user database, the administrator would send spam messages to train-is-spam@example.com and good messages to train-is-not-spam@example.com, from training-group@example.com instead of his own email address.

Similarly, incorrectly classified messages can be submitted to the group/global database by the administrator using the training-group@example 'from' address to prevent these corrections from affecting his personal Bayesian database.

History

FortiMail v3.0	New.

Related topics

- set as profile modify bayesian
- set as profile modify actions

as greylist

Use these command to configure the greylist settings.

Syntax

```
set as greylist capacity <cap_int>
set as greylist exempt {add | delete} <address>
set as greylist greylistperiod <period_int>
set as greylist initial_expiry_period <exp_int>
set as greylist ttl <ttl_int>
```

Keywords and Variables	Description	Default
`capacity <cap_int>`	Use this command to set the maximum number of greylist items stored in the greylist database. New items causing the greylist database to grow larger than the set capacity will overwrite the oldest item. • `<cap_int>` is the maximum number of items in the greylist database. The default value and acceptable range varies by FortiMail model. To display the currently set capacity, use the `get as greylist` command. To determine the available capacity range for your FortiMail model, enter a question mark for the capacity value and execute the command.	varies
`exempt {add | delete} <address>`	Use this command to add or delete addresses from the greylist exemption list. • `<address>` can be an email address, IP address, a subnet, or a domain.	
`greylistperiod <period_int>`	Use this command to set the length of time the FortiMail unit will continue to reject messages with an unknown to/from/IP. After this time expires, any resend attempts will have the to/from/IP data added to the greylist and subsequent messages will be delivered immediately. • `<period_int>` is the greylisting period in minutes. Acceptable values range from 1 to 120 minutes.	`20`
`initial_expiry_period <exp_int>`	Use this command to set the length of time after the initial message that the FortiMail unit will keep record of a message with an unknown to/from/IP. If the mail server resends a message before the initial expiry period expires, it will be accepted. If the message is received after the initial expiry period, the FortiMail treats the delivery as new and rejects the message with a temporary fail. Note that both the greylist period and the initial expiry period are calculated from the time the first message is received and a temporary fail is returned. Consequently, a 20 minute greylist period and a 4 hour initial expiry period will result on a 3 hours and 40 minutes window for delivery of the message to fulfill the greylist requirements and be accepted. • `<exp_int>` is the initial expiry period in hours. Acceptable values range from 4 to 24 hours.	`4`
`ttl <ttl_int>`	Use this command to set the greylist time-to-live (TTL) value. TTL determines how long the to/from/IP data will be retained in the FortiMail unit's greylist. When the entry expires, it is removed and new messages are again rejected until the sending server attempts to deliver the message again. • `<ttl_int>` is the time to live in days. Acceptable values range from 1 to 60 days.	`10`

History

FortiMail v3.0	New.

Related topics

- set as profile modify greylist

as mms_reputation

The MMS Reputation menu enables you to configure MSISDN blacklisting and whitelisting.

When used on a mobile phone network, the FortiMail unit can examine text messages for spam. If a user sends multiple spam messages, all messages from the user will be blocked for a time. The number of spam messages and the length of time further messages will be blocked are configurable.

MSISDN reputation is enabled in the session profile. The auto blacklist score trigger, and the auto blacklist duration are configured in the session profile.

Syntax

```
set as mms_reputation settings autoblacklist window <minutes_int>
```

Keywords and Variables	Description	Default
`window <minutes_int>`	MSISDN reputation functions by detecting whether a sender is responsible for more than a certain number of spam messages within the auto blacklist window duration. This duration is set by specifying the Auto blacklist Window Size in minutes.	`15`

History

FortiMail v3.0 MR4 New.

Related topics

- set ip_profile mms_reputation

as profile delete

Use this command to delete an antispam profile.

Syntax

```
set as profile <name_str> delete
```

`<name_str>` is the name of the profile.

History

FortiMail v3.0	New.

as profile modify actions

Use these commands to modify the actions of an antispam profile.

Reject, discard, and forward are mutually exclusive. No more than one can be enabled at any time. If the specified profile does not exist, it is created.

Syntax

```
set as profile <name_str> modify actions discard {enable | disable}
set as profile <name_str> modify actions emailaddr <address_str>
set as profile <name_str> modify actions forward {enable | disable}
set as profile <name_str> modify actions reject {enable | disable}
set as profile <name_str> modify actions summary {enable | disable}
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the antispam profile.	
`discard {enable | disable}`	Enable or disable discarding spam without sending reject responses to the senders.	`disable`
`emailaddr <address_str>`	Enter the email address to which messages are forwarded when forwarding is enabled.	No default
`forward {enable | disable}`	Enable or disable forwarding of spam messages.	`disable`
`reject {enable | disable}`	Enable or disable the FortiMail unit to reject spam and send reject responses to the sending system.	`disable`
`summary {enable | disable}`	Enable or disable the generation of a report for users who have quarantined spam.	`enable`

History

FortiMail v3.0 New.

Related topics

- set as profile modify quarantine
- set as profile modify individualaction scanner

as profile modify auto-release

Use these commands to configure the auto-release settings for an antispam profile.

Syntax

```
set as profile <name_str> modify auto-release {enable | disable}
  [webrelease {enable | disable} [autowhitelist {enable | disable}]]
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`auto-release {enable | disable}`	Auto-release enables the user to release or delete quarantined spam via email.	`enable`
`webrelease {enable | disable}`	Webrelease enables the user to release or delete quarantined spam via HTTP, with a click from the spam report.	`disable`
`autowhitelist {enable | disable}`	Autowhitelist examines messages the user sends and automatically adds the destination email addresses to their personal white list.	`disable`

History

FortiMail v3.0 New.

Related topics

- set as control autorelease
- set as profile modify quarantine
- set as profile modify whitelistword

as profile modify bannedword

Use this command to enable or disable banned word filtering for the specified profile.

Syntax

```
set as profile <name_str> modify bannedword {enable | disable}
```

`<name_str>` is the name of the profile. By default, banned word scanning is disabled.

History

FortiMail v3.0	New.

Related topics

- set as profile modify bannedwordlist

as profile modify bannedwordlist

Use these commands to modify the banned word list for an antispam profile.

Syntax

```
set as profile <name_str> modify bannedwordlist <word_str> add
set as profile <name_str> modify bannedwordlist <word_str> delete
set as profile <name_str> modify bannedwordlist <word_str> move-to
  <position_int>
set as profile <name_str> modify bannedwordlist <word_str> rename-to
  <new_str>
```

Keywords and variables	Description
`<name_str>`	Enter the name of the antispam profile to modify.
`<word_str>`	The word entry you want to modify in the profile's banned word list.
`add`	Add the new banned word.
`delete`	Delete the banned word.
`move-to <position_int>`	Change the position of the word in the banned word list. Each word is numbered, the first is 1, the second 2, and so on. • `<position_int>` is the word's new position.
`rename-to <new_str>`	Change the word entry.

History

FortiMail v3.0 New.

Related topics

- set as profile modify bannedword

as profile modify bayesian

Use these commands to configure Bayesian spam filtering for an antispam profile.

Syntax

```
set as profile <name_str> modify bayesian autotrain {enable | disable}
set as profile <name_str> modify bayesian scanner {enable | disable}
set as profile <name_str> modify bayesian userdb {enable | disable}
set as profile <name_str> modify bayesian usertrain {enable | disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`autotrain {enable | disable}`	Enable or disable the use of FortiGuard-Antispam and SURBL filtering results to train a user Bayesian database that does not have 200 non-spam email entries and 100 spam entries and is therefore not ready to classify email.	`enable`
`scanner {enable | disable}`	Enable or disable Bayesian filtering for the specified profile.	`disable`
`userdb {enable | disable}`	Enable or disable the use of user Bayesian databases.	`disable`
`usertrain {enable | disable}`	Enable or disable the acceptance of training messages from users.	`enable`

History

FortiMail v3.0 New.

Related topics

- set as control bayesian

as profile modify deepheader

Use this command to enable or disable deep header scanning or for the specified profile. The two separate checks that make up the deep header scan can also be individually enabled or disabled.

Syntax

```
set as profile <name_str> modify deepheader scanner {enable | disable}
set as profile <name_str> modify deepheader checkip {enable | disable}
set as profile <name_str> modify deepheader headeranalysis
  {enable | disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`scanner {enable | disable}`	Enable or disable the deep header scan for the specified profile.	`disable`
`checkip {enable | disable}`	Enable or disable the black IP portion of the deep header scan for the specified profile.	`disable`
`headeranalysis {enable | disable}`	Enable or disable the headers analysis portion of the deep header scan for the specified profile.	`disable`

History

FortiMail v3.0	New.
FortiMail v3.0 MR1	`checkip` and `headeranalysis` added.

Related topics

- set as profile modify actions
- set as profile modify deepheader
- set as profile modify individualaction scanner
- set out_profile profile modify deepheader
- get spam deepheader

as profile modify dictionary

Use these commands to configure dictionary scans for an antivirus profile. If the any of the words appearing in the specified dictionary are detected in an email message, the message is treated as spam.

Syntax

```
set as profile <name_str> modify dictionary dict_profile <dict_int>
set as profile <name_str> modify dictionary scanner {enable | disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`dict_profile <dict_int>`	Select the dictionary profile to be used for dictionary scans. • `<dict_int>` is the dictionary profile number.	No default
`scanner {enable | disable}`	Enable or disable dictionary scanning for the specified profile.	`disable`

History

FortiMail v3.0 New.

Related topics

- set as profile modify actions
- set as profile modify individualaction scanner

as profile modify dnsbl

Use this command to enable or disable communication with the DNSBL servers to scan email for the specified profile. IP addresses defined as private network addresses by RFC 1918 are not checked.

Syntax

```
set as profile <name_str> modify dnsbl {enable | disable}
```

`<name_str>` is the name of the profile. By default, the DNSBL lookup is disabled.

History

FortiMail v3.0	New.

Related topics

- set as profile modify dnsblserver

as profile modify dnsblserver

Use these commands to modify the DNSBL server list for an antispam profile.

Syntax

```
set as profile <name_str> modify dnsblserver <host_str> add
set as profile <name_str> modify dnsblserver <host_str> delete
set as profile <name_str> modify dnsblserver <host_str> move-to <new_int>
set as profile <name_str> modify dnsblserver <host_str> rename-to
  <new_str>
```

Keywords and variables	Description
`<name_str>`	Enter the name of the antispam profile to modify.
`<host_str>`	The DNSBL server entry you want to modify in the profile.
`add`	Add the new DNSBL server.
`delete`	Delete the DNSBL server.
`move-to <new_int>`	Change the position of the DNSBL server in the server list. Each entry is numbered, the first is 1, the second 2, and so on. • `<new_int>` is the entry's new position.
`rename-to <new_str>`	Change the DNSBL server hostname.

History

FortiMail v3.0 New.

Related topics

- set as profile modify dnsbl

as profile modify forgedip

Use this command to enable or disable forged IP checking for an antispam profile.

Syntax

```
set as profile <name_str> modify forgedip {enable | disable}
```

`<name_str>` is the name of the profile. By default, forged IP checking is disabled.

History

FortiMail v3.0	New.

Related topics

- set as profile modify actions
- set as profile modify individualaction scanner

as profile modify fortishield

Use these commands to configure FortiGuard Antispam functions for an antispam profile.

Syntax

```
set as profile <name_str> modify fortishield checkip {enable | disable}
set as profile <name_str> modify fortishield scanner {enable | disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`checkip {enable | disable}`	Enable or disable FortiGuard-Antispam IP address checking for the specified profile. IP addresses defined as private network addresses by RFC 1918 are not checked.	`disable`
`scanner {enable | disable}`	Enable or disable FortiGuard-Antispam scanning for the specified profile.	`disable`

History

FortiMail v3.0	New.

Related topics

- set fshd
- set as profile modify actions
- set as profile modify individualaction scanner
- set fshd

as profile modify greylist

Use this command to enable or disable greylisting for an antispam profile.

Syntax

```
  set as profile <name_str> modify greylist {enable | disable}
```

`<name_str>` is the name of the profile. By default, greylisting is disabled.

History

FortiMail v3.0	New.

Related topics

- set as greylist
- set as profile modify actions
- set as profile modify individualaction scanner

as profile modify heuristic

Use these commands to configure heuristic scanning for an antispam profile.

Syntax

```
set as profile <name_str> modify heuristic lower-level <lower_int>
set as profile <name_str> modify heuristic scanner {enable | disable}
set as profile <name_str> modify heuristic upper-level <upper_int>
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`lower-level <lower_int>`	Enter the lower level threshold for heuristic scanning for the specified profile.	`-20.000000`
`scanner {enable | disable}`	Enable or disable heuristic scanning for the specified profile.	`disable`
`rules-percentage`	Specify the percentage of the total number of heuristic rules that will be used to examine the message. A larger percentage requires more system resources.	`25`
`upper-level <upper_int>`	Enter the upper level threshold for heuristic scanning for the specified profile.	`10.000000`

History

FortiMail v3.0	New.
FortiMail v3.0 MR1	Added `rules-percentage` keyword.

Related topics

- set as profile modify actions
- set as profile modify individualaction scanner

as profile modify imagespam

Use these commands to configure an antispam profile to identify spam messages in which the text is stored as an embedded graphics file.

Syntax

```
set set as profile <name_str> modify imagespam aggressive
   {enable | disable}
set set as profile <name_str> modify imagespam scanner {enable | disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`aggressive {enable | disable}`	Enable or disable more intensive examination of email messages containing images. This option will also force the examination of image file attachments in addition to embedded images. The additional scanning workload could affect performance with traffic containing image files.	`disable`
`scanner {enable | disable}`	Enable or disable scanning of email for image-based spam messages.	`disable`

History

FortiMail v3.0	New.

Related topics

- set as profile modify actions
- set as profile modify individualaction scanner

as profile modify individualaction scanner

Use these commands to set the action each spam detection method takes for messages detected as spam.

Syntax

```
set as profile <name_str> modify individualaction
  [scanner {bannedword |bayesian|deepheader |dictionary | forgedip |
    fortishield | heuristic | imagespam | dnsbl | surbl | virus}]
  [action {default | subject | reject | discard | forward | quarantine}]
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`scanner {bannedword | bayesian | deepheader | dictionary | forgedip | fortishield | heuristic | imagespam | dnsbl | surbl | virus}`	Select the spam detection method.	No default
`action {default | subject | reject | discard | forward | quarantine}`	Select the action to take when spam is detected. • Set `default` to use the default action set with the`set as profile modify actions` command. • Set `subject` to tag the message subject. • Set `reject` to reject the message and return an error to the sending system. • Set `discard` to accept the message and delete it without informing the sending system. • Set `forward` to have messages forwarded to the email address set with the `emailaddr` keyword of the `set as profile modify actions` command. • Set `quarantine` to divert spam to the user's spam quarantine.	`default`

History

FortiMail v3.0	New.

Related topics

- set as profile modify actions

as profile modify quarantine

Use these commands to configure quarantine settings for an antispam profile.

Syntax

```
set as profile <name_str> modify quarantine days <days_int>
set as profile <name_str> modify quarantine queue {enable | disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`days <days_int>`	Enter the number of days to keep the quarantined email for the specified profile. Enter 0 to disable.	`0`
`queue {enable | disable}`	Enable or disable the storage of spam in the quarantine for the specified profile.	`disable`

History

FortiMail v3.0	New.

Related topics

- set as control autorelease
- set as spamreport

as profile modify rewrite_rcpt

The rewrite recipient email address feature allows the FortiMail unit to change the recipient email address if the message is detected as spam. Use these commands to configure the recipient email address rewrite feature.

Syntax

```
set as profile <name_str> modify rewrite_rcpt {enable | disable}
set as profile <name_str> modify rewrite_rcpt set_part {local | domain}
  {none | prefix | replace | suffix} value <rewrite_str>
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`rewrite_rcpt {enable | disable}`	Enable to allow the FortiMail unit to replace the recipient email address if the message is detected as spam.	`disable`
`set_part {local | domain}`	Select the portion of the email address to configure. The changes to the local part (before the '@') and the domain part (after the '@') are configured separately. Note that both parts can be configured separately if changes to both parts are required.	
`{none | prefix | replace | suffix}`	For each part, select: • None: The FortiMail unit will not change the specified part of the email address. • Prefix: The text you specify with the `value` keyword will be added to the beginning of the specified part of the email message. • Suffix: The text you specify with the `value` keyword will be added to the end of the specified part of the email message. • Replace: The text you specify with the `value` keyword will replace the specified part of the email message.	
`value <rewrite_str>`	Enter the text string to be added or used to replace the specified part of the email address. If no message replacement is specified, the value keyword is not necessary.	

History

FortiMail v3.0 MR4 New.

as profile modify scanoptions

Use these commands to configure the antispam scanning options.

Syntax

```
set as profile <name_str> modify scanoptions attachment_type pdf {enable
   | disable}
set as profile <name_str> modify scanoptions bypass_on_auth {enable |
   disable}
set as profile <name_str> modify scanoptions maxsize <size_int>
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`attachment_type pdf {enable | disable}`	Enable to allow the FortiMail unit scan the first page of PDF attachments. The PDF option allows the heuristic, banned word, and image spam scanning techniques to examine the contents of PDF files. If none of these three scanners are enabled, the PDF option will have no effect.	`disable`
`bypass_on_auth {enable | disable}`	Enable or disable the bypassing of spam scanning when an SMTP sender is authenticated.	`disable`
`maxsize <size_int>`	Enter the maximum message size, in bytes, that the FortiMail unit will scan for spam. Messages with sizes exceeding the set limit will not be scanned for spam. Enter 0 to scan all messages regardless of size.	`0`

History

FortiMail v3.0	New.
FortiMail v3.0 MR1	`attachment_type pdf` added.

Related topics

as profile modify surbl

Use this command to enable or disable the checking of mail against defined SURBL servers for an antispam profile.

Syntax

```
set as profile <name_str> modify surbl {enable | disable}
```

`<name_str>` is the name of the profile. By default, SURBL scanning is disabled.

History

FortiMail v3.0	New.

Related topics

- set as profile modify surblserver

as profile modify surblserver

Use these commands to configure the SURBL server list of an antispam profile.

Syntax

```
set as profile <name_str> modify surblserver <host_str> add
set as profile <name_str> modify surblserver <host_str> delete
set as profile <name_str> modify surblserver <host_str> move-to <new_int>
set as profile <name_str> modify surblserver <host_str> rename-to
  <new_str>
```

Keywords and variables	Description
`<name_str>`	Enter the name of the antispam profile to modify.
`<host_str>`	The SURBL server entry you want to modify in the profile.
`add`	Add the new SURBL server.
`delete`	Delete the SURBL server.
`move-to <new_int>`	Change the position of the SURBL server in the server list. Each entry is numbered, the first is 1, the second 2, and so on. `<new_int>` is the entry's new position.
`rename-to <new_str>`	Change the SURBL server hostname.

History

FortiMail v3.0 New.

Related topics

- set as profile modify surbl

as profile modify tags

Use these commands to configure header and subject tagging for an antispam profile.

Syntax

```
set as profile <name_str> modify tags htag <tag_str>
set as profile <name_str> modify tags header {enable | disable}
set as profile <name_str> modify tags stag <tag_str>
set as profile <name_str> modify tags subject {enable | disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`htag <tag_str>`	Enter the text added to the email header.	No default
`header {enable | disable}`	Enable or disable header tagging for the specified profile. A header tag must be set before header tagging can be enabled.	`disable`
`stag <tag_str>`	Enter the text added to the email subject.	No default
`subject {enable | disable}`	Enable or disable subject tagging for the specified profile.	`disable`

History

FortiMail v3.0 New.

Related topics

- set as profile modify actions
- set as profile modify individualaction scanner

as profile modify virus

Use this command to enable or disable treating messages with a virus as spam.

Syntax

```
set as profile <name_str> modify virus {enable | disable}
```

By default, this setting is disabled.

History

FortiMail v3.0	New.

Related topics

- set as profile modify actions
- set as profile modify individualaction scanner

as profile modify whitelistword

Use this command to enable or disable white list word checking in the specified incoming antispam profile.

Syntax

```
set as profile <name_str> modify whitelistword {enable | disable}
```

By default, this setting is disabled.

History

FortiMail v3.0 MR3 New.

Related topics

- set as profile modify whitelistwordlist

as profile modify whitelistwordlist

Use this command to add, delete, or modify white list words for the specified antispam profile.

Syntax

```
set as profile <name_str> modify whitelistwordlist <word_str> add subject
  {enable | disable} body {enable | disable}
set as profile <name_str> modify whitelistwordlist <word_str> change body
  {enable | disable}
set as profile <name_str> modify whitelistwordlist <word_str> change
  subject {enable | disable}
set as profile <name_str> modify whitelistwordlist <word_str> change word
  <new_str>
set as profile <name_str> modify whitelistwordlist <word_str> delete
set as profile <name_str> modify whitelistwordlist <word_str> move-to
  <dest_int>
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`<word_str>`	Enter the whitelist word.	
`add subject {enable	disable} body {enable	disable}`	Add the specified word as a whitelist word. Enable or disable checking of the message subject and body for the whitelist word.	
`change body {enable	disable}`	Select whether the email body text is examined for whitelist words.	`disable`
`change subject {enable	disable}`	Select whether the email subject text is examined for whitelist words.	`disable`
`change word <new_str>`	Change the specified white list word. The `<name_str>` variable specifies the existing word and `<new_str>` is the new word.	
`delete`	Delete the specified whitelist word	
`move-to <dest_int>`	Move the specified word to the position in the white list word list specified by the `<dest_int>` variable.	

History

FortiMail v3.0 MR3 New.

Related topics

- set as profile modify whitelistword

as spamreport

Use these commands to configure spam reports.

Syntax

```
set as spamreport hostname <host_str>
set as spamreport https {enable | disable}
set as spamreport interval <option>
set as spamreport timeofday <time_str>
set as spamreport webaccess_expiry_period <hours_int>
```

Keywords and variables	Description	Default
`hostname <host_str>`	Enter an alternate resolvable host name to use if the local domain name is not resolvable from everywhere users will receive their mail.	
`https {enable | disable}`	Enable or disable encrypted communication between the user and the FortiMail unit when the user selects a release or delete link in an HTML formatted spam quarantine report.	`enable`
`interval {thesedays <day_int> | thesehours <hours_int>}`	Specify how often spam reports will be generated and sent to users. The two options work together and both need to be set. • `{thesedays}` allows you to specify on which days spam reports will be generated. The `<day_int>` variable specifies the days, separated by commas. Sunday through Saturday are represented by the digits 0 through 6. For example, Sunday is 0, Tuesday is 2, Friday is 5. To specify reports generated Monday through Friday, the command line would be: `set as spamreport interval thesedays 1,2,3,4,5` • `{thesehours}` will specify what times of the day spam reports will be generated. The `<hours_int>` variable specifies the hours, separated by commas. For example, to define the hourly generation of spam reports during business hours, the command line would be: `set as spamreport interval thesehours 9,10,11,12,13,14,15,16,17` The two example command lines given direct the FortiMail unit to generate a spam report every hour from 9 A.M. to 5 P.M., Monday to Friday.	
`webaccess_expiry_period <hours_int>`	Specify the number of hours a user will be able to use the link in the spam report to access his spam quarantine without providing a username and password. If the link is used after the configured number of hours, the users will be informed that the link has expired and redirected to the quarantine login page. Enter 0 to always require the user enter a username and password. Valid values are 0 to 720.	`0`

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Added `webaccess_expiry_period`. Removed `timeofday`. Removed `daily` and `weekly` options, and added `thesedays` option to `interval` keyword.

Related topics

- set as control autorelease
- set as profile modify quarantine

as trusted

Use these commands to configure trusted MTA addresses. If there are any servers within your network that mail travels through before reaching the FortiMail unit, the addresses of these servers would be checked as part of the antispam scans. If spam mail cannot be introduced by these servers, you can exclude them from the antispam checks.

Antispam scanning methods that observe these trusted addresses include FortiGuard Antispam, DNSBL, SPF, and DKIM.

Private network addresses are never checked and do not need to be excluded using this command.

Syntax

```
set as trusted antispam-mta add <ipv4_mask>
set as trusted antispam-mta delete <ipv4_mask>
set as trusted mta add <ipv4_mask>
set as trusted mta delete <ipv4_mask>
```

Keywords and variables	Description	Default
`antispam-mta add <ipv4_mask>`	Enter an IP address/mask to add to the FortiMail unit's antispam-MTA list. Addresses on this list are the points past which no addresses will be scanned for spam. For example, if a server is at the very edge of your network and no servers inside your network will generate spam, use the `antispam-mta add` command to specify the server at the edge of the network. Once done, the IP address of the specified server, and all servers between it and the FortiMail unit will be ignored for antispam scans.	
`antispam-mta delete <ipv4_mask>`	Enter an IP address/mask to delete from the antispam MTA list.	
`mta add <ipv4_mask>`	Enter an IP address/mask to add to the FortiMail unit's MTA list. Addresses on this list will be ignored by certain FortiMail antispam scans.	
`mta delete <ipv4_mask>`	Enter an IP address/mask to delete from the MTA list.	

History

FortiMail v3.0 MR3 New.

Related topics

- set as profile modify fortishield
- set as profile modify dnsbl
- set ip_profile sendervalidation

auth imap rename-to

Use this command to rename an IMAP authentication profile.

Syntax

```
set auth imap <name_str> rename-to <new_str>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the IMAP authentication profile.	
`<new_str>`	Enter the new name of the IMAP authentication profile.	

History

FortiMail v3.0	New.

Related topics

- set auth imap server

auth imap server

Use this command to create or modify the server properties of an IMAP authentication profile.

Syntax

```
set auth imap <name_str> server {<host_str> | <server_ipv4>} port
  <port_int> [option {ssl secure tls domain}]
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the IMAP authentication profile.	
`{<host_str> | <server_ipv4>}`	Enter either the IMAP server host name or IP address.	
`port <port_int>`	Enter the IMAP server port number.	389 for non-secure connections. 636 for secure connections.
`[option {ssl secure tls domain}]`	These optional settings further define the connection to the IMAP server. • `{ssl}` enables Secure Sockets Layer (SSL) on the IMAP server to secure message transmission. • `{secure}` enables Secure Authentication on the IMAP server to secure email users passwords. • `{tls}` enables Transport Layer Security (TLS) on the IMAP server to ensure privacy between communicating applications and their users on the Internet. • `{domain}` select if the IMAP server requires the domain for authentication.	

History

FortiMail v3.0 New.

Related topics

- set auth imap rename-to

auth pop3 rename-to

Use this command to rename a POP3 authentication profile.

Syntax

```
set auth pop3 <name_str> rename-to <new_str>
```

Keywords and Variables	Description
`<name_str>`	This is the name of the POP3 authentication profile.
`<new_str>`	Enter the new name of the POP3 authentication profile.

History

FortiMail v3.0	New.

Related topics

- set auth pop3 server

auth pop3 server

Use this command to create or modify the server properties of an POP3 authentication profile

Syntax

```
set auth pop3 <name_str> server {<host_str> | <server_ipv4>} port
  <port_int> [option {ssl secure tls domain}]
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the POP3 authentication profile.	
`{<host_str> | <server_ipv4>}`	Enter either the POP3 server host name or IP address.	
`port <port_int>`	Enter the POP3 server port number.	`110`
`[option {ssl secure tls domain}]`	These optional settings further define the connection to the POP3 server. • `{ssl}` enables Secure Sockets Layer (SSL) on the POP3 server to secure message transmission. • `{secure}` enables Secure Authentication on the POP3 server to secure email users passwords. • `{tls}` enables Transport Layer Security (TLS) on the POP3 server to ensure privacy between communicating applications and their users on the Internet. • `{domain}` select if the POP3 server requires the domain for authentication.	

History

FortiMail v3.0 New.

Related topics

- set auth pop3 rename-to

auth radius rename-to

Use this command to rename a Radius authentication profile.

Syntax

```
set auth radius <name_str> rename-to <new_str>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the Radius authentication profile.	No default
`<new_str>`	Enter the new name of the Radius authentication profile.	No default

History

FortiMail v3.0	New.

Related topics

- set auth radius server

auth radius server

Use this command to create or modify the server properties of a Radius authentication profile.

Syntax

```
set auth radius <name_str> server {<host_str> | <server_ipv4>} secret
  <password_str> domain {enable | disable}
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the Radius authentication profile.	
`{<host_str> | <server_ipv4>}`	Enter either the Radius server host name or IP address.	
`secret <password_str>`	Enter the password required to access the Radius server.	
`domain {enable | disable}`	Select `enable` if the server requires the domain name in addition to the user ID.	

History

FortiMail v3.0 New.

Related topics

- set auth radius rename-to

auth smtp rename-to

Use this command to rename an SMTP authentication profile.

Syntax

```
set auth smtp <name_str> rename-to <new_str>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the SMTP authentication profile.	
`<new_str>`	Enter the new name of the SMTP authentication profile.	

History

FortiMail v3.0	New.

Related topics

- set auth smtp server

auth smtp server

Use this command to create or modify the server properties of an SMTP authentication profile.

Syntax

```
set auth smtp <name_str> server {<host_str> | <server_ipv4>} port
  <port_number> [option {ssl secure tls domain}]
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the SMTP authentication profile.	
`{<host_str> | <server_ipv4>}`	Enter either the SMTP server host name or IP address.	
`port <port_int>`	Enter the SMTP server port number.	25
`[option {ssl secure tls domain}]`	These optional settings further define the connection to the SMTP server. • `{ssl}` enables Secure Sockets Layer (SSL) on the SMTP server to secure message transmission. • `{secure}` enables Secure Authentication on the SMTP server to secure email users passwords. • `{tls}` enables Transport Layer Security (TLS) on the SMTP server to ensure privacy between communicating applications and their users on the Internet. • `{domain}` select if the SMTP server requires the domain for authentication.	

History

FortiMail v3.0	New.

Related topics

- set auth smtp rename-to

av delete

Use this command to delete antivirus profiles.

Syntax

```
set av <av_prof_name> delete
```

where `<av_prof_name>` is the name of an antivirus profile.

History

FortiMail v3.0	New.

Related topics

- set alertemail deferq
- set av modify heuristic
- set av modify heuristic heuristic_action
- set av rename-to

av modify actions

Use this command to select, for a specified antivirus profile, the action taken when the FortiMail unit detects an infected email message. Specify `reject` to reject the email message and return an error. Specify `discard` to simply discard the message after receipt.

Syntax

```
set av <av_prof_name> modify actions {discard | reject}
```

`<av_prof_name>` is the name of the antivirus profile you are configuring. If this is not the name of an existing profile, a new profile is created.

History

FortiMail v3.0	New.

Related topics

- set alertemail configuration mailto
- set av modify heuristic
- set av modify heuristic heuristic_action
- set alertemail setting option
- set av rename-to

av modify heuristic

Use this command to enable or disable heuristic scanning for the specified antivirus profile.

Syntax

```
set av <av_prof_name> modify heuristic {enable | disable}
```

`<av_prof_name>` is the name of the antivirus profile you are configuring. If this is not the name of an existing profile, a new profile is created.

History

FortiMail v3.0	New.

Related topics

- set alertemail configuration mailto
- set alertemail deferq
- set av modify heuristic heuristic_action
- set alertemail setting option
- set av rename-to

av modify heuristic heuristic_action

Use this command to specify how this antivirus profile handles email messages that contain an infected attachment, as detected through heuristics. The options are:

- Disable both `discard` and `reject`. FortiMail replaces the infected attachment.
- Enable `discard`. FortiMail discards the message after receipt.
- Enable `reject`. FortiMail rejects the email message and returns an error to the sending server.

You cannot enable both `discard` and `reject`. Enabling one disables the other.

Syntax

To disable both `discard` and `reject`:

```
set av <av_prof_name> modify heuristic heuristic_action discard disable
set av <av_prof_name> modify heuristic heuristic_action reject disable
```

To enable `discard`:

```
set av <av_prof_name> modify heuristic heuristic_action discard enable
```

To enable `reject`:

```
set av <av_prof_name> modify heuristic heuristic_action reject enable
```

`<av_prof_name>` is the name of the antivirus profile you are configuring. If this is not the name of an existing profile, a new profile is created.

History

FortiMail v3.0	New.

Related topics

- set alertemail configuration mailto
- set alertemail deferq
- set av modify heuristic
- set alertemail setting option
- set av rename-to

av modify scanner

Use this command to enable or disable antivirus scanning for the specified profile.

Syntax

```
set av <av_prof_name> modify scanner {enable | disable}
```

`<av_prof_name>` is the name of the antivirus profile you are configuring. If this is not the name of an existing profile, a new profile is created.

History

FortiMail v3.0	New.

Related topics

- set alertemail configuration mailto
- set alertemail deferq
- set av modify heuristic
- set av modify heuristic heuristic_action
- set av rename-to

av rename-to

Use this command to enable or disable antivirus scanning for the specified profile.

Syntax

```
set av <av_prof_name> rename-to <newname_str>
```

`<av_prof_name>` is the name of the antivirus profile to rename. `<newname_str>` is the new name.

History

FortiMail v3.0	New.

Related topics

- set alertemail configuration mailto
- set alertemail deferq
- set av modify heuristic heuristic_action
- set alertemail setting option

console

Use `set console` to configure console settings.

Syntax

```
set console baudrate {9600 | 19200 | 38400 | 57600 | 115200}
  mode {batch | line} page <line_int>
```

Commands	**Description**
`baudrate {9600 | 19200 | 38400 | 57600 | 115200}`	Sets the console baudrate.
`mode {batch | line}`	Sets the console mode to batch or line. The default setting is line.
`page <line_int>`	Sets the number of lines that appear on each page of command line console output. The default setting is 25. You can set this value to 0 to allow output to flow without paging. • `<line_int>` is the number of lines that appear on each page of command line console output.

History

FortiMail v3.0 New.

Related topics

- set system appearance
- set system option

content delete

Use this command to delete a content profile.

Syntax

```
set content <name_str> delete
```

`<name_str>` is the name of the content profile.

History

FortiMail v3.0	New.

Related topics

- set content modify filetype
- set content modify monitor

content modify action

Use this command to select the action to be taken on messages matching the specified content profile.

Syntax

```
set content <name_str> modify action {treat_as_spam | reject| discard |
  replace | quarantine | forward} [forwardaddr <addr_str>]
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the content profile.	
`action {discard	forward	quarantine	reject	replace	treat_as_spam}`	Select the action to be taken on messages matching the active content profile. • `{discard}` deletes the message. • `{forward}` sends the message to the specified email address instead of the recipient • `{quarantine}` stores the infected message in the FortiMail unit's system quarantine. This option is available for incoming email only. • `{reject}` causes the FortiMail unit to not accept delivery of the infected message. An error is returned to the system attempting delivery. • `{replace}` strips the infected attachment and replaces it with the a custom message. • `{treat_as_spam}` handles the infected message according to the action set in the applicable antispam profile.	`replace`
`forwardaddr <addr_str>`	Enter the email address to be used if the selected action is forward. When forward is selected as the action, matching messages will be forwarded to the specified email address.	

History

FortiMail v3.0 New.

Related topics

- set content modify filetype
- set content modify monitor

content modify bypass_on_auth

Use this command to allow messages to bypass the content filters if SMTP authorization is enabled and the delivering system successfully authenticates.

Syntax

```
set content <name_str> modify bypass_on_auth {enable | disable}
```

`<name_str>` is the name of the content profile.

History

FortiMail v3.0	New.

Related topics

- set content modify action
- set content modify filetype

content modify defersize

Use this command to set the minimum size of files that will be held for later content scanning.

Syntax

```
set content <name_str> modify defersize <size_int>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the content profile.	
`<size_int>`	Enter the size limit (in KB). Files larger than the set limit will be deferred. A value of 0 means no mail will be deferred.	`0`

History

FortiMail v3.0	New.

Related topics

- set content modify bypass_on_auth
- set content modify filetype

content modify filetype

Use this command to block email attachments that match the specified file type.

Syntax

```
set content <name_str> modify filetype <filetype_str> {blocked |
  not-blocked}
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the content profile.	
`<filetype_str>`	Select the file type. Valid types are • `video` • `audio` • `image` • `application/executable` • `application/document` • `application/archive` • `application/other` This option includes all file types not specified by the other listed types.	
`{blocked | not-blocked}`	Select `blocked` to trigger the content action against messages containing the specified type of file attachment. Select `not-blocked` to allow the specified type of file attachment.	`not-blocked`

History

FortiMail v3.0	New.

Related topics

- set content modify action
- set content modify monitor

content modify monitor

Use this command to configure content monitor profiles.

Syntax

```
set content <name_str> modify monitor <profile_int> delete
set content <name_str> modify monitor <profile_int> dict_profile
  <dict_int>
set content <name_str> modify monitor <profile_int> {enable | disable}
set content <name_str> modify monitor <profile_int> moveto <new_int>
set content <name_str> modify monitor <profile_int> tags header {enable |
  disable}
set content <name_str> modify monitor <profile_int> tags htag <tag_str>
set content <name_str> modify monitor <profile_int> tags stag <tag_str>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the content profile.	
`<profile_int>`	Enter the content monitor profile number.	
`<dict_int>`	Enter the dictionary profile ID number to use for the specified content monitor profile.	
`{enable | disable}`	Enable or disable the specified content monitor profile.	`enable`
`moveto <new_int>`	Moves the specified content monitor profile to a new position in the list. • `<new_int>` is the destination content profile number.	
`tags header {enable | disable}`	Enable or disable the labeling of matching messages by adding a tag to the header.	`disable`
`tags htag <tag_str>`	Enter the text to be used as the tag when header tagging is enabled.	
`tags subject {enable | disable}`	Enable or disable the labeling of matching messages by adding a tag to the subject.	`disable`
`tags stag <tag_str>`	Enter the text to be used as the tag when subject tagging is enabled.	

History

FortiMail v3.0 New.

Related topics

- set content modify monitor action

content modify monitor action

Use this command to select the action to be taken with messages matching the specified content monitor profile.

Syntax

```
set content <name_str> modify monitor <profile_int> action {none |
  discard | forward | quarantine | reject | replace | review |
  treat_as_spam}
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the content profile.	
`<profile_int>`	Enter the content monitor profile number.	
`action {none | discard | forward | quarantine | reject | replace | review | treat_as_spam}`	Select the action to be taken with messages matching the specified content monitor profile. • `{none}` no action is taken, though subject and/or header tagging will still occur if enabled. • `{discard}` deletes the message. • `{forward}` sends the message to the specified email address instead of the recipient. • `{quarantine}` stores the infected message in the FortiMail unit spam quarantine. • `{reject}` causes the FortiMail unit to not accept delivery of the infected message. An error is returned to the system attempting delivery. • `{replace}` strips the infected attachment and replaces it with the a custom message. • `{review}` stops messages matching the monitor profile and places them into the system quarantine. These messages are not included in the spam report sent to users. Rather, an administrator must release or delete these messages after reviewing them. • `{treat_as_spam}` handles the infected message according to the action set in the applicable antispam profile.	none

History

FortiMail v3.0	New.

Related topics

- set content modify monitor

fshd

Use `set fshd` to configure FortiGuard service on the FortiMail unit.

Syntax

```
set fshd cache status {enabled | disabled}
set fshd cache ttl <ttl_int>
set fshd hostname <hostname_str>
set fshd status {enabled | disabled}
```

.

Commands	Description	Default
`cache status {enabled | disabled}`	Enables or disables the FortiGuard cache.	`enabled`
`cache ttl <ttl_int>`	Sets a TTL (time to live) for the cache. `<ttl_int>` is the number of seconds blocked IP addresses are stored in the FortiMail unit's cache before contacting the FortiGuard server again.	`600`
`hostname <hostname_str>`	Sets the FortiGuard server host name.	antispam.fortigate.com
`status {enabled | disabled}`	Enables or disables FortiGuard service.	`enabled`

History

FortiMail v3.0	New.

ip_policy

Use this command to create a new IP policy.

Policies are referenced by number, indicating their position in the policy list. Numbering starts with 0 for the first policy. New policies must be created at the end of the current list (the next number in sequence).

Syntax

```
set ip_policy <policy_int>
```

`<policy_int>` is the IP policy number.

History

FortiMail v3.0	New.

Related topics

- set ip_policy delete
- set ip_policy move

ip_policy action

Use this command to set the default action to be applied to a connection matching the specified IP policy.

Syntax

```
set ip_policy <policy_int> action {scan | reject | tempfail}
```

Keywords and Variables	Description	Default
`<policy_int>`	This is IP policy number.	
`scan`	Select scan to allow the connection and apply the antispam, antivirus, auth, content, and session (IP) profiles associated with the IP policy.	`scan`
`reject`	Select reject to have the FortiMail unit reject connection attempts matching this policy.	
`tempfail`	Select tempfail to have the FortiMail unit reject connection attempts and report a temporary failure.	

History

FortiMail v3.0	New.

Related topics

- set ip_policy as
- set ip_policy auth
- set ip_policy av
- set ip_policy content
- set ip_policy ip

ip_policy as

Use this command to set the antispam profile to be applied to traffic controlled by the specified IP policy.

Syntax

```
set ip_policy <policy_int> as <name_str>
```

Keywords and Variables	Description
`<policy_int>`	Enter the IP policy number.
`<name_str>`	Enter the name of the antispam profile.

History

FortiMail v3.0	New.

Related topics

- set ip_policy auth
- set ip_policy av
- set ip_policy content
- set ip_policy ip

ip_policy auth

Use this command to set the authentication type and profile to be applied to the specified IP policy.

Syntax

```
set ip_policy <policy_int> auth imap <name_str>
set ip_policy <policy_int> auth pop3 <name_str>
set ip_policy <policy_int> auth radius <name_str>
set ip_policy <policy_int> auth smtp <name_str>
```

Keywords and Variables	Description
`<policy_int>`	Enter the IP policy number.
`<name_str>`	Enter the name of the authentication profile.

History

FortiMail v3.0	New.

Related topics

- set ip_policy as
- set ip_policy av
- set ip_policy content
- set ip_policy ip

ip_policy av

Use this command to set the antivirus profile to be applied to traffic controlled by the specified IP policy.

Syntax

```
set ip_policy <policy_int> av <name_str>
```

Keywords and Variables	Description
`<policy_int>`	Enter the IP policy number.
`<name_str>`	Enter the name of the antivirus profile.

History

FortiMail v3.0	New.

Related topics

- set ip_policy as
- set ip_policy auth
- set ip_policy content
- set ip_policy ip

ip_policy content

Use this command to set the antivirus profile to be applied to traffic controlled by the specified IP policy.

Syntax

```
set ip_policy <policy_int> content <name_str>
```

Keywords and Variables	Description
`<policy_int>`	Enter the IP policy number.
`<name_str>`	Enter the name of the content profile.

History

FortiMail v3.0	New.

Related topics

- set ip_policy as
- set ip_policy auth
- set ip_policy av
- set ip_policy ip

ip_policy delete

Use this command to delete an IP policy.

Policies are referenced by number, indicating their position in the policy list. Numbering starts with 0 for the first policy.

Syntax

```
set ip_policy <policy_int> delete
```

`<policy_int>` is the IP policy number.

History

FortiMail v3.0	New.

Related topics

- set ip_policy
- set ip_policy move

ip_policy exclusive

Use this command to disable any checks for recipient-based policy matches while this IP-based policy is in effect. The IP-based profile will be applied and matching recipient-based profiles ignored.

Syntax

```
set ip_policy <policy_int> exclusive {enable | disable}
```

`<policy_int>` is the IP policy number.

History

FortiMail v3.0	New.

Related topics

- set ip_policy match (gateway and server modes)
- set ip_policy match (transparent mode)

ip_policy ip

Use this command to set the session profile to be applied to the specified IP policy.

Syntax

```
set ip_policy <policy_int> ip <name_str>
```

Keywords and variables	Description	Default
`<policy_int>`	Enter the IP policy number.	
`<name_str>`	Enter the name of the session profile.	`session_strict`

History

FortiMail v3.0	New.

Related topics

- set ip_policy as
- set ip_policy auth
- set ip_policy av
- set ip_policy content

ip_policy match (gateway and server modes)

Use this command to set the client IP address. The IP policy applies to traffic exchanged when this client establishes a connection.

Syntax

```
set ip_policy <policy_int> match <client_ipv4/mask>
```

Keywords and variables	Description	Default
`<policy_int>`	Enter the IP policy number.	
`<client_ipv4/mask>`	Enter the IP address and CIDR subnet of the client. The address 0.0.0.0/0 will include all addresses.	`0.0.0.0/0`

History

FortiMail v3.0	New.

Related topics

- set ip_policy match (transparent mode)

ip_policy match (transparent mode)

Use this command to set the client and server IP addresses. The IP policy applies to traffic exchanged when the client connected to the server.

In the context of this command, the client is the system initiating the connection and the server is the system receiving the connection attempt.

Syntax

```
set ip_policy <policy_integer> match <client_ipv4/mask>
  <server_ipv4/mask>
```

Keywords and variables	Description	Default
`<policy_int>`	Enter the IP policy number.	
`<client_ipv4/mask>`	Enter the IP address and CIDR subnet of the client. The address 0.0.0.0/0 will include all addresses.	`0.0.0.0/0`
`<server_ipv4/mask>`	Enter the IP address and CIDR subnet of the server. The address 0.0.0.0/0 will include all addresses.	`0.0.0.0/0`

History

FortiMail v3.0	New.

Related topics

- set ip_policy match (gateway and server modes)

ip_policy move

Use this command to move an IP-based policy from one position in the list to another.

Syntax

```
set ip_policy <policy_int> move <new_int>
```

Keywords and variables	Description	Default
`<policy_int>`	Enter the IP policy number.	
`<new_int>`	Enter the IP policy’s new number. The new policy number is the position to where you want to move the IP policy.	

History

FortiMail v3.0	New.

Related topics

- set ip_policy
- set ip_policy delete

ip_policy smtp

Use this command to configure the use of other authentication types for SMTP.

Syntax

```
set ip_policy <policy_integer> smtp {enable | disable}
set ip_policy <policy_integer> smtp enable [{enable | disable}]
```

Keywords and variables	Description
`<policy_int>`	Enter the IP policy number.
`{enable | disable}`	Enable or disable the use of the authentication type defined in the authentication profile for SMTP authentication.
`[{enable | disable}]`	If authentication is enabled, choose to enable or disable the sender being allowed to have a different name than their SMTP sender identity.

History

FortiMail v3.0	New.

Related topics

- set ip_policy auth

ip_pool

Use this command to add create a new IP pool profile.

Syntax

```
set ip_pool <name_str>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the IP pool profile to create.	

History

FortiMail v3.0 MR3 New.

Related topics

- set ip_pool add_entry
- set ip_pool del_entry
- set ip_pool delete
- get ip_pool

ip_pool add_entry

Use this command to add a range of IP addresses to an IP pool profile.

Syntax

```
set ip_pool <name_str> add_entry <ipv4> <size_int>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the IP pool profile.	
`<ipv4>`	Enter the Start IP address for the range of IP addresses in this IP pool.	
`<size_int>`	Enter the Range Size. This is the number of available IP addresses starting with the Start IP address.	

History

FortiMail v3.0 MR3	New.

Related topics

- set ip_pool
- set ip_pool del_entry
- set ip_pool delete
- get ip_pool

ip_pool del_entry

Use this command to delete an IP address range from an IP pool profile.

Syntax

```
set ip_pool <name_str> del_entry <rangeID_int>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the IP pool profile.	
`<rangeID_int>`	Enter the ID number of the IP range to be deleted. Use the `get ip_pool` command to list the defined ranges with their IDs.	

History

FortiMail v3.0 MR3	New.

Related topics

- set ip_pool
- set ip_pool add_entry
- set ip_pool delete
- get ip_pool

ip_pool delete

Use this command to delete an IP pool profile.

Syntax

```
set ip_pool <name_str> delete
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the IP pool profile.	

History

FortiMail v3.0 MR3 New.

Related topics

- set ip_pool
- set ip_pool add_entry
- set ip_pool del_entry
- get ip_pool

ip_profile check

Use these commands to configure various session checks.

Syntax

```
set ip_profile <name_str> check 3_way {enable | disable}
set ip_profile <name_str> check allow_pipelining {no | loose | strict}
set ip_profile <name_str> check domain {enable | disable}
set ip_profile <name_str> check eom_ack {enable | disable}
set ip_profile <name_str> check helo {enable | disable}
set ip_profile <name_str> check open_relay {enable | disable}
set ip_profile <name_str> check recipient {enable | disable}
set ip_profile <name_str> check rewrite_helo {enable | disable}
set ip_profile <name_str> check rewrite_helo_custom {enable | disable}
  <helo_str>
set ip_profile <name_str> check send_dsn {enable | disable}
set ip_profile <name_str> check sender {enable | disable}
set ip_profile <name_str> check splice {enable | disable} <integer>
  {seconds | kilobytes}
set ip_profile <name_str> check stop_empty_domains {enable | disable}
set ip_profile <name_str> check stop_encrypted {enable | disable}
set ip_profile <name_str> check syntax {enable | disable}
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the session profile.	
`3_way {enable | disable}`	Enable or disable message rejection if recipient and HELO domain match but sender domain is different. This check only affects unauthenticated sessions.	`disable`
`allow_pipelining {no | loose | strict}`	Disable, enable, or enable strict command pipelining. • `{no}` The FortiMail unit accepts only a single command at a time during an SMTP session. • `{loose}` Some SMTP command sequences are accepted and processed as a group, increasing performance over high-latency connections. • `{strict}` Pipelining is enabled, but limited to strict compliance with RFC-2920.	`no`
`domain {enable | disable}`	Enable or disable rejection of EHLO/HELO commands with invalid characters in the domain.	`disable`
`eom_ack {enable | disable}`	Enable or disable immediately acknowledging end of message (EOM) signal. If disabled, the antispam check is run on the message before acknowledgement is sent. The sending server could time-out while waiting for EOM acknowledgement.	`disable`
`helo {enable | disable}`	Enable to disable checking of the existence of the domain reported in the client's HELO command by looking up both the MX record and A record.	`disable`
`open_relay {enable | disable}`	Enable or disable open relay check. This check only affects unauthenticated sessions.	`disable`
`recipient {enable | disable}`	Enable or disable checking the recipient address for a valid domain.	`disable`
`rewrite_helo {enable | disable}`	Enable or disable rewriting the EHLO/HELO domain to the IP string of the client address. The rewritten EHLO/HELO will be in the format x.x.x.x	`disable`
`rewrite_helo_custom {enable | disable} <helo_str>`	Select to rewrite the HELO domain to the specified value for any session this profile applies to.	`disable`

Keywords and Variables	Description	Default
`send_dsn {enable | disable}`	Enable or disable the sending of a delivery status notification (DSN) message to the sender when spam is detected	`disable`
`sender {enable | disable}`	Enable or disable checking of the recipient for an invalid domain. This check only affects unauthenticated sessions.	`disable`
`splice {enable | disable} <integer> {seconds | kilobytes}`	Enable or disable the switching to splice mode after a specified amount of data is transmitted or time has passed. • `<integer>` is the number of kilobytes or seconds.	`disable`
`stop_empty_domains {enable | disable}`	Enable or disable rejection of empty domains. This check only affects unauthenticated sessions.	`disable`
`stop_encrypted {enable | disable}`	Enable or disable preventing encrypted communication sessions. Encrypted email cannot be scanned for spam or viruses.	`disable`
`syntax {enable | disable}`	Enable or disable the enforcement of strict syntax checking.	`disable`

History

FortiMail v3.0 New.

Related topics

- set ip_profile connection
- set ip_profile error
- set ip_profile limit
- set ip_profile list
- set ip_profile senderreputation

ip_profile connection

Use these commands to configure various session connection attributes.

Syntax

```
set ip_profile <name_str> connection concurrent <con_int>
set ip_profile <name_str> connection hide {enable | disable}
set ip_profile <name_str> connection idle_timeout <int>
set ip_profile <name_str> connection rate <con_int> <time_int>
set ip_profile <name_str> connection stop_blacklisted {enable | disable}
set ip_profile <name_str> connection total <con_int>
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the session profile.	
`concurrent <con_int>`	Enter the maximum allowed number of concurrent connections to each client. Additional connections are rejected. • `<con_int>` is the maximum number of concurrent connections allowed to each client. Enter 0 to disable limiting.	`0`
`hide {enable | disable}`	When enabled, no information will be added to email message headers to indicate the FortiMail unit has intercepted, examined, and perhaps processed the message. This option appears only in transparent mode.	`disable`
`idle_timeout <int>`	Enter the number of seconds after which an inactive connection will be dropped. • `<int>` is the timeout in seconds. Enter 0 to disable timeout.	`0`
`rate <con_int> <time_int>`	Enter the number of connection allowed per client during a user-defined time frame. • `<con_int>` is the number of connections. • `<time_int>` is the time in minutes. Enter 0 connections and 0 minutes to disable limiting.	`0`
`stop_blacklisted {enable | disable}`	Enable or disable the relaying of email to blacklisted servers. The active antispam detection methods determine blacklisting which addresses are blacklisted.	`disable`
`total <con_int>`	Enter the maximum number of concurrent connections. Enter 0 to disable limiting.	`0`

History

FortiMail v3.0	New.

Related topics

- set ip_profile check
- set ip_profile error
- set ip_profile limit
- set ip_profile list
- set ip_profile senderreputation

ip_profile delete

Use this command to delete a session profile.

Syntax

```
set ip_profile <name_str> delete
```

`<name_str>` is the name of the profile.

History

FortiMail v3.0	New.

Related topics

- set ip_profile rename

ip_profile error

Use these commands to set the parameters related to session communication error penalties.

Syntax

```
set ip_profile <name_str> error free <int>
set ip_profile <name_str> error initial_delay <int>
set ip_profile <name_str> error increment <int>
set ip_profile <name_str> error total <int>
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the session profile.	
`free <int>`	Enter the number of ‘free’ errors allowed in a communication session. The FortiMail unit will begin to penalize the client when the number of errors exceed this free threshold.	1
`initial_delay <int>`	Enter the number of seconds the communication session is delayed when the first ‘non-free’ error occurs.	4
`increment <int>`	Enter the number of seconds added to the delay for each additional ‘non-free’ error.	4
`total <int>`	Enter the total number of errors (both free and non-free) allowed before the session is terminated.	5

History

FortiMail v3.0 New.

Related topics

- set ip_profile check
- set ip_profile connection
- set ip_profile limit
- set ip_profile list
- set ip_profile senderreputation

ip_profile headermanipulation

Use these commands to have the FortiMail unit remove headers you specify from email messages.

Syntax

```
set ip_profile <name_str> headermanipulation remove_received {enable |
  disable}
set ip_profile <name_str> headermanipulation remove_header {enable |
  disable}
set ip_profile <name_str> headermanipulation headerlist add <key_str>
set ip_profile <name_str> headermanipulation headerlist delete <key_str>
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the session profile.	
`remove_received {enable | disable}`	Enable to remove the received headers from email messages. If the messages move through any email servers after the FortiMail unit, these mail servers will add their own received headers.	`disable`
`remove_header {enable | disable}`	Enter to remove from email messages any headers defined with the `headerlist add` command.	`disable`
`headerlist add <key_str>`	Enter a header key (the portion of the header before the colon) to have the FortiMail unit remove the header when `remove_header` is enabled.	
`headerlist delete <key_str>`	Enter a header key to remove it from the header list. Once removed, the remove header command will not affect the header you remove.	

History

FortiMail v3.0 MR4 New.

Related topics

- set ip_profile check
- set ip_profile connection
- set ip_profile error
- set ip_profile list
- set ip_profile senderreputation

ip_profile limit

Use these commands to set the parameters related to session communication limits.

Syntax

```
set ip_profile <name_str> limit noop <int>
set ip_profile <name_str> limit rset <int>
set ip_profile <name_str> limit emails <int>
set ip_profile <name_str> limit header_size <int>
set ip_profile <name_str> limit helo <int>
set ip_profile <name_str> limit message_size <int>
set ip_profile <name_str> limit recipients <int>
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the session profile.	
`noop <int>`	Enter the maximum number of SMTP NOOPs allowed before the connection is dropped.	`10`
`rset <int>`	Enter the maximum number of SMTP resets allowed before the connection is dropped.	`20`
`emails <int>`	Enter the maximum number of email messages exchanged during the communication session.	`10`
`header_size <int>`	Enter the maximum permitted email message header size, in bytes. If larger, the header will be truncated.	`32768`
`helo <int>`	Enter the maximum number of EHLO/HELOs permitted per session.	`3`
`message_size <int>`	Enter the maximum permitted email message size, in bytes. If larger, the message will be truncated.	`10485760`
`recipients <int>`	Enter the maximum number of recipients permitted per email message.	`500`

History

FortiMail v3.0	New.

Related topics

- set ip_profile check
- set ip_profile connection
- set ip_profile error
- set ip_profile list
- set ip_profile senderreputation

ip_profile list

Use these commands to enable or disable the session white and black lists.

Syntax

```
set ip_profile <name_str> list black {enable | disable}
set ip_profile <name_str> list to_black {enable | disable}
set ip_profile <name_str> list to_white {enable | disable}
set ip_profile <name_str> list white {enable | disable}
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the session profile.	
`black {enable | disable}`	Enable or disable sender black list checking for the specified session profile.	`disabled`
`to_black {enable | disable}`	Enable or disable recipient black list checking for the specified session profile.	`disabled`
`to_white {enable | disable}`	Enable or disable recipient white list checking for the specified session profile.	`disabled`
`white {enable | disable}`	Enable or disable sender white list checking for the specified session profile.	`disabled`

History

FortiMail v3.0	New.

Related topics

- set ip_profile check
- set ip_profile connection
- set ip_profile error
- set ip_profile limit
- set ip_profile senderreputation

ip_profile mms_reputation

The MMS Reputation menu enables you to configure MSISDN blacklisting and whitelisting.

When used on a mobile phone network, the FortiMail unit can examine text messages for spam. If a user sends multiple spam messages, all messages from the user will be blocked for a time. The number of spam messages and the length of time further messages will be blocked are configurable.

MSISDN reputation Auto blacklist Window Size is enabled in the antispam settings

Syntax

```
set ip_profile test mms_reputation {enable | disable}
set ip_profile test mms_reputation autoblacklist duration {0 | 15 | 30 |
  60 | 120 | 240 | 480 | 1440}
set ip_profile test mms_reputation autoblacklist trigger <trigger_int>
```

Keywords and Variables	Description	Default
`mms_reputation {enable | disable}`	Enable MSISDN reputation checking for traffic examined by the session profile.	`disable`
`autoblacklist duration {0 | 15 | 30 | 60 | 120 | 240 | 480 | 1440}`	When blacklisted, messages from a sender will be blocked for the configured number of minutes.	`0`
`autoblacklist trigger <trigger_int>`	Automatically add the sender to the auto blacklist when the configured number of messages are detected as spam within the auto blacklist window time period.	5

History

FortiMail v3.0 MR4 New.

Related topics

- set as mms_reputation

ip_profile rename

Use this command to rename an existing session profile.

Syntax

```
set ip_profile <name_str> rename <new_str>
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the session profile.	
`rename <new_str>`	Enter the new name of the specified session profile.	

History

FortiMail v3.0	New.

Related topics

- set ip_profile delete

ip_profile senderreputation

Use these commands to configure the sender reputation feature.

Syntax

```
set ip_profile <name_str> senderreputation reject <int>
set ip_profile <name_str> senderreputation status {enable | disable}
set ip_profile <name_str> senderreputation tempfail <int>
set ip_profile <name_str> senderreputation throttle <int>
set ip_profile <name_str> senderreputation throttle_number <int>
set ip_profile <name_str> senderreputation throttle_percent <int>
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the session profile.	
`reject <int>`	Enter the sender reputation reject threshold. If a system's sender reputation score exceeds this value, connection attempts by the system will be refused with a reject error.	`80`
`status {enable | disable}`	Enable or disable sender reputation score calculation and actions for the specified session profile.	`disable`
`tempfail <int>`	Enter the sender reputation tempfail threshold. If a system's sender reputation score exceeds this value, connection attempts by the system will be refused with a tempfail error.	`55`
`throttle <int>`	Enter the sender reputation throttle threshold. If a system's sender reputation score exceeds this value, the number of messages the FortiMail unit will accept from the sender is limited to the number permitted by the `throttle_number` or `throttle_percent`, whichever is larger.	`15`
`throttle_number <int>`	Enter the number of messages per hour accepted from a throttled sender.	`1`
`throttle_percent <int>`	Sets the number of messages per hour accepted from a throttled sender, expressed as a percentage of the number of messages from the same sender in the previous hour.	`5`

History

FortiMail v3.0	New.

Related topics

- set ip_profile check
- set ip_profile connection
- set ip_profile error
- set ip_profile limit
- set ip_profile list

ip_profile sendervalidation

The sender validation options allow confirmation of sender and message validity.

Syntax

```
set ip_profile <name_str> sendervalidation authenticated {enable |
  disable}
set ip_profile <name_str> sendervalidation bypassbounceverify {enable |
  disable}
set ip_profile <name_str> sendervalidation dkim {enable | disable}
set ip_profile <name_str> sendervalidation domainkey {enable | disable}
set ip_profile <name_str> sendervalidation signing {enable | disable}
set ip_profile <name_str> sendervalidation spf {enable | disable}
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the session profile.	
`authenticated {enable | disable}`	Only available when DKIM signing is enabled, this setting will limit DKIM message signing to senders who authenticate with the FortiMail unit.	`disable`
`bypassbounceverify {enable | disable}`	If bounce verification is enabled, select bypass bounce verification for connections matching this policy. This bypass does not prevent the tagging of outgoing messages. For information on enabling verification of delivery status notification (DSN) email, see "as bounceverify" on page 99.	`disable`
`dkim {enable | disable}`	Check the validity of DKIM signatures, if present. An invalid signature will increase 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 validation is skipped.	`disable`
`domainkey {enable | disable}`	If the sender domain DNS record lists DomainKeys authorized IP addresses, the DomainKeys check will compare the client IP address to the authorized senders. A DomainKeys failure increases the client sender reputation score. A DomainKeys validation decreases the client sender reputation score. If the sender domain DNS record does not publish DomainKeys information, the check is skipped.	`disable`
`signing {enable | disable}`	Sign outgoing messages with DKIM signatures. Signed messages can be validated at their destination. Signing requires that a domain key selector be generated by the FortiMail unit and added to the DNS zone file. The domain key selector can be generated in the domain configuration. Go to Mail Settings > Domains > Domains.	`disable`
`spf {enable | disable}`	If the sender domain DNS record lists SPF authorized IP addresses, the SPF check will compare the client IP address to the authorized senders. An SPF failure increases the client sender reputation score. An SPF validation decreases the client sender reputation score. If the sender domain DNS record does not publish SPF information, the check is skipped.	`disable`

History

FortiMail v3.0	New.
FortiMail v3.0 MR4	Added keyword `bypassbounceverify`.

Related topics

- set ip_profile check
- set ip_profile connection
- set ip_profile error
- set ip_profile limit
- set ip_profile list

ip_profile_setting rate_control

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.

Syntax

```
set ip_profile_setting rate_control {connection | message}
```

Keywords and Variables	Description	Default
`rate_control {connection | message}`	The Fortimail unit can control email traffic by either the number of connections or by the number of email messages. • **connection** allows you to specify the maximum number of connections from each IP address within a specified number of minutes. • **message** allows you to specify the maximum number of email messages accepted from each IP address within a specified number of minutes.	`connection`

History

FortiMail v3.0 MR4 New.

ldap_profile profile asav

Use these commands to enable the FortiMail unit to query an LDAP server for user antivirus and antispam parameters.

Syntax

```
set ldap_profile profile <name_str> asav antispam <as_str>
set ldap_profile profile <name_str> asav antivirus <av_str>
set ldap_profile profile <name_str> asav asavstate {enable | disable}
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the LDAP profile.	
`antispam <as_str>`	Set the LDAP antispam on/off attribute.	no default
`antivirus <av_str>`	Set the LDAP antivirus on/off attribute	no default
`asavstate {enable | disable}`	Enable or disable the LDAP antispam/antivirus attribute configuration.	`disable`

History

FortiMail v3.0 New.

Related topics

- set as profile modify actions
- set av modify actions
- unset ldap_profile

ldap_profile clearallcache

Use this command to clear all LDAP profile caches.

Syntax

```
set ldap_profile clearallcache
```

History

FortiMail v3.0 MR3 New.

Related topics

- set ldap_profile profile clearcache
- set ldap_profile profile option
- unset ldap_profile

ldap_profile profile auth

Use these commands to configure the way the way users are authenticated.

Syntax

```
set ldap_profile profile <name_str> auth authstate {enable | disable}
set ldap_profile profile <name_str> auth cnidname <cnid_str>
set ldap_profile profile <name_str> auth cnidstatus {enable | disable}
set ldap_profile profile <name_str> auth searchstatus {enable | disable}
set ldap_profile profile <name_str> auth upnstatus {enable | disable}
set ldap_profile profile <name_str> auth upnsuffix <upns_str>
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the LDAP profile.	
`authstate {enable | disable}`	Enable or disable the user authentication options.	`disable`
`cnidname <cnid_str>`	Set the common name identifier.	`uid`
`cnidstatus {enable | disable}`	Enable or disable the common name identifier.	`enable`
`searchstatus {enable | disable}`	Enable or disable the search.	`disable`
`upnstatus {enable | disable}`	Enable or disable the UPN.	`disable`
`upnsuffix <upns_str>`	Set an alternate UPN suffix.	no default

History

FortiMail v3.0	New.

Related topics

- set ldap_profile profile group
- set ldap_profile profile option
- set ldap_profile profile pwd
- set ldap_profile profile routing
- set ldap_profile profile server
- set ldap_profile profile user
- unset ldap_profile

ldap_profile profile clearcache

Use this command to clear the cache of the specified LDAP profile.

Syntax

```
set ldap_profile profile <name_str> clearcache
```

History

FortiMail v3.0 MR3 New.

Related topics

- set ldap_profile clearallcache
- set ldap_profile profile auth
- set ldap_profile profile group
- set ldap_profile profile option
- set ldap_profile profile pwd
- set ldap_profile profile routing
- set ldap_profile profile server
- set ldap_profile profile user
- unset ldap_profile

ldap_profile profile fallback_server

Use this command to configure an LDAP fallback server. If the server defined in the Server Name/IP field is unreachable and a fallback server is defined, the FortiMail unit will connect to the fallback server to submit its query. To clear the fallback server, issue the command with an empty server name as shown in the syntax examples.

Syntax

```
set ldap_profile profile <name_str> fallback_server {<host_str> |
  <server_ipv4>} port <port_int>
  set ldap_profile profile <name_str> fallback_server ''
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the LDAP profile.	
`fallback_server {<host_str>	<server_ipv4>}`	Set fallback LDAP server address by specifying a hostname or IP address.	No default.
`port <port_int>`	Enter the port used to communicate with the fallback LDAP server.	389

History

FortiMail v3.0 MR3 New.

Related topics

- set ldap_profile clearallcache
- set ldap_profile profile auth
- set ldap_profile profile clearcache
- set ldap_profile profile pwd
- set ldap_profile profile routing
- set ldap_profile profile server
- set ldap_profile profile user
- unset ldap_profile

ldap_profile profile group

Use these commands to configure an LDAP group query.

Syntax

```
set ldap_profile profile <name_str> group groupstate {enable | disable}
set ldap_profile profile <name_str> group groupstate {enable | disable}
  virtual {enable | disable} memberofattribute <attr_str> relativename
  {enable | disable} basedn <basedn_str> groupnameattribute <grp_str>
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the LDAP profile.	
`groupstate {enable | disable}`	Enable or disable group LDAP queries.	`disable`
`virtual {enable | disable}`	Enable this option to specify any LDAP tree node. Any node that falls under the specified tree node will be considered a member of the group. Since the specified node isn't defined as a group in the LDAP database, the FortiMail unit sees it as a sort of 'virtual group.'	`disable`
`membershipattribute <attr_str>`	Enter the user attribute that defines the groups the user belongs to. For example, this attribute is `memberOf` for Active Directory servers.	
`relativename {enable | disable}`	With the appropriate information entered, the admin need only enter the LDAP group name when creating a recipient-based policy, for example. If this option is disabled, the group name attribute, group name, and group base DN must be specified in the policy.	`disable`
`basedn <basedn_str>`	Enter the group base DN if `relativename` is enabled.	
`groupnameattribute <grp_str>`	Enter the group name attribute if `relativename` is enabled.	

History

FortiMail v3.0 MR3 New.

Related topics

- set ldap_profile clearallcache
- set ldap_profile profile auth
- set ldap_profile profile clearcache
- set ldap_profile profile pwd
- set ldap_profile profile routing
- set ldap_profile profile server
- set ldap_profile profile user
- unset ldap_profile

ldap_profile profile option

Use these commands to configure the advanced LDAP profile options.

Syntax

```
set ldap_profile profile <name_str> option cachestate {enable | disable}
set ldap_profile profile <name_str> option cachettl <ttl_int>
set ldap_profile profile <name_str> option timelimit <timeout_int>
set ldap_profile profile <name_str> option unauthbind {enable | disable}
set ldap_profile profile <name_str> option version {ver2 | ver3}
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the LDAP profile.	
`cachestate {enable | disable}`	Enable or disable the LDAP cache. The FortiMail unit will cache LDAP queries to reduce the amount of network traffic by eliminating redundant queries. Select Clear Cache to clear the LDAP queries the FortiMail unit has saved.	`disable`
`cachettl <ttl_int>`	Enter the amount of time, in minutes, the FortiMail unit will cache LDAP queries. When the configured time elapses after the query is submitted, the saved query is cleared from the cache.	`1440`
`timelimit <timeout_int>`	Set the length of time, in seconds, the FortiMail unit will wait for a submitted search to return a result.	`10`
`unauthbind {enable | disable}`	Enable or disable unauthenticated LDAP binds.	`disable`
`version {ver2 | ver3}`	Set the version of the protocol used to communicate with the LDAP server.	`ver3`

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Added `cachestate` and `cachettl`.

Related topics

- set ldap_profile clearallcache
- set ldap_profile profile auth
- set ldap_profile profile clearcache
- set ldap_profile profile fallback_server
- set ldap_profile profile group
- set ldap_profile profile pwd
- set ldap_profile profile routing
- set ldap_profile profile server
- set ldap_profile profile user
- unset ldap_profile

ldap_profile profile pwd

Use these commands to configure webmail password options.

Syntax

```
set ldap_profile profile <name_str> pwd webmailschema {openldap |
  activedirectory | <schema_str>}
set ldap_profile profile <name_str> pwd webmailstatus {enable | disable}
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the LDAP profile.	
`webmailschema {openldap | activedirectory | <schema_str>}`	Set the webmail password change schema. • `{openldap}` is the openldap schema. • `{activedirectory}` is the Active Directory schema. • `<schema_str>` allows you to enter a custom schema of your choice.	`openldap`
`webmailstatus {enable | disable}`	Enable or disable the webmail password change.	`disable`

History

FortiMail v3.0	New.

Related topics

- set ldap_profile profile auth
- set ldap_profile profile group
- set ldap_profile profile option
- set ldap_profile profile routing
- set ldap_profile profile server
- set ldap_profile profile user
- unset ldap_profile

ldap_profile profile routing

Use these commands to configure mail routing options if each user’s LDAP profile contains mail routing information.

Syntax

```
set ldap_profile profile <name_str> routing addr <route_str>
set ldap_profile profile <name_str> routing host <host_str>
set ldap_profile profile <name_str> routing routingstate {enable |
  disable}
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the LDAP profile.	
`addr <route_str>`	Set the LDAP routing mailrouting address attribute.	`mailRoutingAddress`
`host <host_str>`	Set the LDAP routing mailrouting host attribute.	`mailHost`
`routingstate {enable | disable}`	Enable or disable the LDAP routing configuration.	`disable`

History

FortiMail v3.0 New.

Related topics

- set ldap_profile profile auth
- set ldap_profile profile fallback_server
- set ldap_profile profile group
- set ldap_profile profile option
- set ldap_profile profile pwd
- set ldap_profile profile server
- set ldap_profile profile user
- unset ldap_profile

ldap_profile profile server

Use these commands to configure information about the LDAP server.

Syntax

```
set ldap_profile profile <name_str> server {<host_str> | <server_ipv4>}
  [port <port_int> [secure {none | ssl}]]
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the LDAP profile.	
`server {<host_str> | <server_ipv4>}`	Set LDAP server address by specifying a hostname or IP address.	No default.
`port <port_int>`	Enter the port used to communicate with the LDAP server.	389
`secure {none | ssl}`	Select whether to use a secure (SSL) or non-secure connection to the LDAP server.	none

History

FortiMail v3.0	New.

Related topics

- set ldap_profile profile auth
- set ldap_profile profile fallback_server
- set ldap_profile profile group
- set ldap_profile profile option
- set ldap_profile profile pwd
- set ldap_profile profile routing
- set ldap_profile profile user
- unset ldap_profile

ldap_profile profile user

Use these commands to configure user query options for the FortiMail unit to query the LDAP server.

Syntax

```
set ldap_profile profile <name_str> user basedn <basedn_str>
  set ldap_profile profile <name_str> user binddn <binddn_str>
  set ldap_profile profile <name_str> user bindpw <bindpw_str>
  set ldap_profile profile <name_str> user query <query_str>
  set ldap_profile profile <name_str> user schema {activedirectory |
    dominoperson | inetlocalmailrcpt | inetorgperson | userdefined}
  set ldap_profile profile <name_str> user scope {one | sub}
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the name of the LDAP profile.	
`basedn <basedn_str>`	Enter the distinguished name (DN) that will be the default point from which LDAP directory lookups will occur.	no default
`binddn <binddn_str>`	Enter the bind DN of an account with the rights to complete the required LDAP queries.	no default
`bindpw <bindpw_str>`	Enter the bind password.	no default
`deref {never | always | search | find}`	Specify how alias dereferencing is done. The values are `Never`, `Always`, `Search`, or `Find` to specify that aliases are never dereferenced, always dereferenced, dereferenced when searching, or dereferenced only when finding the base object for the search.	`never`
`query <query_str>`	Set the query to be used for finding a user in the LDAP directory.	`(& (objectClass =inetOrgPerson) (mail=$m))`
`schema {activedirectory | dominoperson | inetlocalmailrcpt | inetorgperson | userdefined}`	Set the predefined directory schema depending on your LDAP server type. • `{userdefined}` uses the schema set with the user query command.	`inetorgperson`
`scope {one | sub}`	Set the search scope. This setting determines the depth of search. • `{one}` is a single level. • `{sub}` is the subtree.	`sub`

History

FortiMail v3.0 New.

Related topics

- set ldap_profile profile auth
- set ldap_profile profile group
- set ldap_profile profile option
- set ldap_profile profile pwd
- set ldap_profile profile routing
- set ldap_profile profile server

- unset ldap_profile

limits domain-level

Use this command to fine tune the domain-related maximum values on your FortiMail unit.

The syntax requires that the four values be entered every time the command is executed. Even if you only want to change one value, all four must be entered. Entering 0 for any value resets it to the default.

The new values will take effect when the FortiMail unit is restarted.

Syntax

```
set limits domain-level <admin_int> <admin_per_dom_int> <policy_int>
  <profile_int>
```

Keywords and Variables	Description	Default
`<admin_int>`	Enter the maximum number of domains that can have domain-level administrators. More domains can be created, but only the number entered here can have domain-level administrators.	
`<admin_per_dom_int>`	Enter the maximum number of domain-level administrators allowed in each domain.	
`<policy_int>`	Enter the maximum number of domain-specific policies that can be created for each domain.	
`<profile_int>`	Enter the maximum number of domain specific profiles that can be created for each domain. This number is the maximum for each type, not all types together. For example, if the value is set to 10, there can be 10 antispam profiles, 10 session profiles, 10 LDAP profiles, and so on.	

History

FortiMail v3.0 MR3 New.

Related topics

- set limits system-level general
- set limits system-level groups
- set limits system-level mail-users
- set limits system-level other-profiles
- set limits system-level policies
- get limits

limits system-level general

Use this command to fine tune the general system maximum values on your FortiMail unit.

The syntax requires the three values be entered every time the command is executed. Even if you only want to change one value, all three must be entered. Entering 0 for any value resets it to the default.

The new values will take effect when the FortiMail unit is restarted.

Syntax

```
set limits system-level general <admin_int> <domain_int> <profiles_int>
```

Keywords and Variables	Description	Default
`<admin_int>`	Enter the maximum number of system-level admin users that can be created.	
`<domain_int>`	Enter the maximum number of domains that can be created.	
`<profiles_int>`	Enter the maximum number of profiles that can be created.	

History

FortiMail v3.0 MR3 New.

Related topics

- set limits domain-level
- set limits system-level groups
- set limits system-level mail-users
- set limits system-level other-profiles
- set limits system-level policies
- get limits

limits system-level groups

Use this command to fine tune the group-related maximum values on your FortiMail unit.

The syntax requires the two values be entered every time the command is executed. Even if you only want to change one value, both must be entered. Entering 0 for any value resets it to the default.

The new values will take effect when the FortiMail unit is restarted.

Syntax

```
set limits system-level groups <groups_int> <members_int>
```

Keywords and Variables	Description	Default
`<groups_int>`	Enter the maximum number of groups that can be created.	
`<members_int>`	Enter the maximum number of members that can be added to each group.	

History

FortiMail v3.0 MR3 New.

Related topics

- set limits domain-level
- set limits system-level general
- set limits system-level mail-users
- set limits system-level other-profiles
- set limits system-level policies
- get limits

limits system-level mail-users

Use this command to adjust the maximum number of mail users that can be created on your FortiMail unit.

The new value will take effect when the FortiMail unit is restarted.

Syntax

```
set limits system-level mail-users <users_int>
```

Keywords and Variables	Description	Default
`<users_int>`	Enter the maximum number of mail users that can be created.	

History

FortiMail v3.0 MR3 New.

Related topics

- set limits domain-level
- set limits system-level general
- set limits system-level groups
- set limits system-level other-profiles
- set limits system-level policies
- get limits

limits system-level other-profiles

Use this command to fine tune some of the profile-related maximum values on your FortiMail unit.

The syntax requires that the five values be entered every time the command is executed. Even if you only want to change one value, all five must be entered. Entering 0 for any value resets it to the default.

The new values will take effect when the FortiMail unit is restarted.

Syntax

```
set limits system-level other-profiles <as_int> <av_int> <misc_int>
  <content_int> <session_int>
```

Keywords and Variables	Description	Default
`<as_int>`	Enter the maximum number of antispam profiles that can be created.	
`<av_int>`	Enter the maximum number of antivirus profiles that can be created.	
`<misc_int>`	Enter the maximum number of misc profiles that can be created.	
`<content_int>`	Enter the maximum number of content profiles that can be created.	
`<session_int>`	Enter the maximum number of session profiles that can be created.	

History

FortiMail v3.0 MR3 New.

Related topics

- set limits domain-level
- set limits system-level general
- set limits system-level groups
- set limits system-level mail-users
- set limits system-level policies
- get limits

limits system-level policies

Use this command to fine tune the policy-related maximum values on your FortiMail unit.

The syntax requires the two values be entered every time the command is executed. Even if you only want to change one value, both must be entered. Entering 0 for any value resets it to the default.

The new values will take effect when the FortiMail unit is restarted.

Syntax

```
set limits system-level policies <ip_int> <outgoing_int>
```

Keywords and Variables	Description	Default
`<ip_int>`	Enter the maximum number of IP-based policies that can be created.	
`<outgoing_int>`	Enter the maximum number of outgoing recipient-based policies that can be created.	

History

FortiMail v3.0 MR3 New.

Related topics

- set limits domain-level
- set limits system-level general
- set limits system-level groups
- set limits system-level mail-users
- set limits system-level other-profiles
- get limits

log msisdn

Use this command to display the MSISDN column in **Log & Report** > **Logging,** in the web-based manager. The MSISDN column displays only when this command is enabled.

Syntax

To enable the MSISDN column to display in **Log & Report** > **Logging**

```
set log msisdn {enable | disable}
```

History

FortiMail v3.0 MR3 New.

Related topics

- set log view fields

log policy destination event

Use this command to enable and log events to a device. You need to enable event logging before selecting what events to log to a device.

Syntax

To enable and configure events for a device

```
set log policy destination {console | local | syslog} event status enable
set log policy destination {console | local | syslog} event category
  [configuration ha imap login pop3 smtp system updatefailed
  updatesucceeded webmail none]
```

Keywords/Variables	Description	Default
`status {enable | disable}`	Enable or disable event log output to a device.	`disable`
`category [configuration login system updatefailed updatesucceeded smtp ha webmail pop3 imap none]`	Event logging must be enabled for this settings to be applicable. • `[configuration]` log all management events, such as configuration changes. • `[ha]` log all HA events. • `[imap]` log all IMAP events. This selection is only available in server mode. • `[login]` log all administrative events, such as user logins, resets, and configuration updates. • `[pop3]` log all POP3 events. This selection is only available in server mode. • `[smtp]` log all SMTP server events. • `[system]` log all system-related events, such as system restarts. • `[updatefailed]` log all failed update events. • `[updatesucceeded]` log all successful update events. • `[webmail]` log all webmail events. • `[none]` to clear all event categories, specify `none` without any other event categories.	`OFF`

History

FortiMail v2.8 New.

Related topics

- set log setting local
- set log setting syslog
- set log policy destination spam
- set log policy destination virus
- set log policy destination history
- set log view fields
- set log view loglevel

log policy destination history

Use this command to enable history logs to a device.

Syntax

To enable history logs

```
set log policy destination {console | local | syslog} history status
  enable
```

Keywords/Variables	Description	Default
`status {enable	disable}`	Enable or disable history log output to a device.	`disable`

History

FortiMail v2.8	New.

Related topics

- set log setting localset
- set log setting syslog
- set log policy destination event
- set log policy destination spam
- set log policy destination virus
- set log view fields
- set log view loglevel

log policy destination spam

Use this command to enable and log spam events for a device. You need to enable spam logging before selecting spam events.

Syntax

To enable logging of spam events for a device

```
set log policy destination {console | local | syslog} spam status enable
set log policy destination {console | local | syslog} spam category
  detected
```

Keywords/Variables	Description	Default
`{enable	disable}`	Enable or disable spam detection log output to a device.	`disable`
`{detected	none}`	Spam logging must be enabled to be applicable. • `{detected}` log all instances of detected spam messages. • `{none}` to clear all event categories, specify none without any other event categories.	`OFF`

History

FortiMail v2.8	New.

Related topics

- set log setting localset
- set log setting syslog
- set log policy destination event
- set log policy destination virus
- set log policy destination history
- set log view fields
- set log view loglevel

log policy destination virus

Use this command to enable and log virus events for a device. You need to enable virus logging before selecting virus events.

Syntax

To enable logging of virus events for a device

```
set log policy destination {console | local | syslog} virus status enable
set log policy destination {console | local | syslog} virus category
  infected
```

Keywords/Variables	Description	Default
`{enable | disable}`	Enable or disable virus log output to a device.	`disable`
`{infected | none}`	Virus logging must be enabled for these settings to be applicable. • `{infected}` log all instances of virus-infected messages. • `{none}` to clear all event categories, specify none without any other event categories.	`OFF`

History

FortiMail v2.8 New.

Related topics

- set log setting localset
- set log setting syslog
- set log policy destination event
- set log policy destination spam
- set log policy destination history
- set log view fields
- set log view loglevel

log reportconfig direction

Use this command to configure what types of emails the report will contain.

Syntax

To configure the report direction

```
set log reportconfig <reportconfigname> direction {both | incoming |
  outgoing}
```

Keywords/Variables	Description	Default
`{both	incoming	outgoing}`	Select if the information includes incoming email, outgoing email, or both.	`both`

History

FortiMail v2.8 New.

Related topics

- set log setting localset
- set log setting syslog
- set log reportconfig domain
- set log reportconfig mailto
- set log reportconfig period
- set log reportconfig qry
- set log reportconfig schedule hour

log reportconfig domain

Use this command to configure what domain or domains the report will contain.

Syntax

To configure the report domain

```
set log reportconfig <reportconfigname> domain <ALL>
set log reportconfig <reportconfigname> domain <domain_name1>
  [<domain_name2>, <domain_name3>,...]
```

Keywords/Variables	Description	Default
`<ALL>`	Select if you want all domains present in the report.	`ALL`
`<domain_name1> [<domain_name2>, <domain_name3>, ....]`	Select if you want a certain domain or certain domains in the report.	No default

History

FortiMail v2.8	New.

Related topics

- set log setting localset
- set log setting syslog
- set log reportconfig direction
- set log reportconfig mailto
- set log reportconfig period
- set log reportconfig qry
- set log reportconfig schedule hour

log reportconfig mailto

Use this command to configure the email addresses you want to send the generated report to.

Syntax

To configure the email addresses to send the generated report to

```
set log reportconfig <reportconfigname> mailto <email_addr1>
  [<email_addr2>, <email_addr3> ...] format {html | pdf}
```

Keywords/Variables	Description	Default

`<email_addr1>`
`[<email_addr2>,`
`<email_addr3>, ....]`
	Selects the email addresses of recipients who you want the report sent to and the output format of the report.	No default

`format {html | pdf}`	Selects the format the report will be in when sent to the email address.	`pdf`

History

FortiMail v2.8	New.
FortiMail 3.0MR1	Added `format {html | pdf}` keyword.

Related topics

- set log setting localset
- set log setting syslog
- set log reportconfig direction
- set log reportconfig domain
- set log reportconfig period
- set log reportconfig qry
- set log reportconfig schedule hour

log reportconfig period

Use this command to configure the time frame of logs you want included in the report.

Syntax

To configure the period of time for the report

```
set log reportconfig <reportconfigname> period from <YYYY-MM-DD-HH> to
  <YYYY-MM-DD-HH>
set log reportconfig <reportconfigname> period {quarter | month | week |
  <integer> hours | <integer> days | <integer> weeks}
set log reportconfig <reportconfigname> period {year | quarter | month |
  week}
set log reportconfig <reportconfigname> period {today | yesterday}
```

Keywords/Variables	Description	Default
`from <YYYY-MM-DD-HH> to <YYYY-MM-DD-HH>`	Selects the log period of the report by specifying a start and end date and time. The time can only be specified to the nearest hours.	No default
`period {quarter | month | week | <integer> hours | <integer> days | <integer> weeks}`	Selects the log period of the report by specifying a number of hours, days, or weeks leading up to the current time, or the last week, month, or quarter.	No default
`period {year | quarter | month | week}`	Selects the log period of the report by specifying the current year, quarter, month or week.	No default
`period {today | yesterday}`	Selects the log period of the report by specifying the current or previous day.	No default

History

FortiMail v2.8	New.

Related topics

- set log setting localset
- set log setting syslog
- set log reportconfig direction
- set log reportconfig domain
- set log reportconfig mailto
- set log reportconfig qry
- set log reportconfig schedule hour

log reportconfig qry

Use this command to enable the type of query you want included in the report, such as email statistic messages by day.

Syntax

To enable queries for the report

```
set log reportconfig <reportconfigname> <qry> [<query_str1>,
  <query_str2>, <query_str3>, ....] {enable | disable}
```

Keywords/Variables	Description	Default
`<qry> [<query_str1>, <query_str2>, <query_str3>, ....] {enable | disable}`	Enable to include the specified query type in the report. Enter ? at the end of the command syntax to list all the query types, the sets they belong to, and the current status of each.	`disable`

History

FortiMail v2.8	New.

Related topics

- set log setting localset
- set log setting syslog
- set log reportconfig direction
- set log reportconfig domain
- set log reportconfig mailto
- set log reportconfig period
- set log reportconfig schedule hour

log reportconfig schedule hour

Use this command to schedule when the report is automatically generated.

Syntax

To configure the schedule

```
set log reportconfig <reportconfigname> schedule hour {daily | days
  <days_str> | dates <dates_integer>}
set log reportconfig <reportconfigname> schedule off
```

Keywords/Variables	Description	Default
`schedule hour {daily	days <days_str>	dates <dates_int>}`	Configures when scheduled reports are automatically generated. Reports can be scheduled daily, for certain days of the week, for certain dates of each month, or disabled entirely. • `<hour_integer>` is the hour of the day the schedule report is generated. The hour can be 0 to 23, where 0 is midnight at the start of the day. • `<days_str>` is the day or days of the week when the report is automatically generated. Specify days using their first three letters. Any number of days may be entered, separated by commas with no spaces. • `<dates_int>` is the date or dates of the month when the report is automatically generated. Any number of dates may be entered, separated by commas with no spaces.	No default
`off`	Disables scheduling entirely if only on-demand reports are necessary.	`off`

History

FortiMail v2.8 New.

Related topics

- set log setting localset
- set log setting syslog
- set log reportconfig direction
- set log reportconfig domain
- set log reportconfig mailto
- set log reportconfig period
- set log reportconfig qry

log setting console

Use this command to configure logging to the console.

Syntax

To configure logging to the console

```
set log setting console status {enable | disable}
set log setting console loglevel <severity_integer>
```

Keywords/Variables	Description	Default
`status {enable | disable}`	Enable or disable logging to the console.	`disable`
`loglevel <severity_integer>`	Sets the log severity level for the logging device. Use the ? to list the following log levels: 0=Emergency 1=Alert 2=Critical 3=Error 4=Warning 5=Notification 6=Information Logs will include items of the level you set and higher. Set level to 6 if you want to include all log severity levels.	`Emergency`

History

FortiMail v2.8 New.

Related topics

- set log setting local
- set log setting syslog
- set log policy destination event
- set log policy destination spam
- set log policy destination virus
- set log policy destination history

log setting local

Use this command to configure logging to the local FortiMail hard disk.

Syntax

To configure logging to the local hard disk

```
set log setting local status {enable | disable}
set log setting local diskfull {overwrite | nolog}
set log setting local filesz <file-sz_integer>
set log setting local logtime <days_integer>
```

Keywords/Variables	Description	Default
`status {enable | disable}`	Enable or disable logging to a destination.	`disable`
`loglevel <severity_integer>`	Sets the destination log severity level. Use the ? to list the following log levels: 0=Emergency 1=Alert 2=Critical 3=Error 4=Warning 5=Notification 6=Information Logs include items of the level you set and higher. Set level to 6 if you want to include all log severity levels.	`Emergency`
`diskfull {overwrite | nolog}`	Sets the action to take with additional logs when the FortiMail hard disk runs out of space: • `overwrite` deletes the oldest log file when the hard disk is full • `nolog` stops logging messages when the hard disk is full.	`overwrite`
`filesz <file-sz_integer>`	Sets a maximum log file size in Mbytes. When the log file reaches the size, the current log file is closed and saved. A new active log file is then started. The default log file is 10 MB and the maximum allowed size is 1000 MB	`10`
`logtime <days_integer>`	Sets a log time interval in days. At the specified interval, the current log file is closed and saved, and a new one started. The default log time interval is 10 days.	`10`

History

FortiMail v2.8	New.

Related topics

- set log setting syslog
- set log policy destination event
- set log policy destination spam
- set log policy destination virus
- set log policy destination history

log setting syslog

Use this command to configure logging to the Syslog server.

Syntax

To configure logging to the Syslog server

```
set log setting syslog status {enable | disable}
set log setting syslog server <server_ip4>
set log setting syslog port <port_integer>
set log setting syslog number <number_integer>
set log setting syslog csv {enable | disable}
set log setting syslog loglevel <severity_integer>
set log setting syslog facility {alert | audit | auth | authpriv | clock
  | cron | daemon | ftp | kern | lpr | mail | news | netp | local10 |
  local 1 | local2 | local3| local4 | local5 | local6 | local7}
```

Keywords/Variables	Description	Default
`status {enable | disable}`	Enable or disable logging to the remote syslog server.	`disable`
`server <server_ip4>`	Sets the remote host, syslog server, IP address.	No default
`port <port_integer>`	Sets the port number for logging to the Syslog server.	514
`number <number_integer>`	Sets what syslog server receives logs sent from the FortiMail unit. When you use `number`, you need to include the server IP address when entering a number. For example, `set log setting syslog number 2 server 172.20.16.155`.	No default
`csv {enable | disable}`	Enable or disable formatting for CSV format.	`disable`
`loglevel <severity_integer>`	Sets the log severity level for the logging device. Use the ? to list the following log levels: 0=Emergency 1=Alert 2=Critical 3=Error 4=Warning 5=Notification 6=Information Logs will include items of the level you set and higher. Set level to 6 if you want to include all log severity levels.	`Emergency`
`facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kern | lpr | mail | news } netp | local10 | local 1 | local2 | local3| local4 | local5 | local6 | local7}`	Sets the facility identifier used for all log entries sent to the syslog server by the FortiMail unit. Facility can help identify the source of log entries on the syslog server.	`kern`

History

FortiMail v2.8	New.
FortiMail 3.0MR1	Added `number` keyword.

Related topics

- set log setting localset
- set log policy destination event
- set log policy destination spam
- set log policy destination virus
- set log policy destination history

log view fields

Use this command to configure what columns will appear when viewing a log type in the web-based manager.

Syntax

To set the columns to display for a log type

```
set log view {event | history | spam | virus} fields {date time others
  action from log_id module msg pri reason status src_ip submodule
  subtype to type ui user classifier client_name disposition
  message_length resolved session_id subject virus mailer MSISDN}
```

Keywords/Variables	Description	Default
`view {event	history	spam	virus}`	Sets the log type that you want to view in the web-based manager.	No default
`fields {date time others action from log_id module msg pri reason status src_ip submodule subtype to type ui user classifier client_name disposition message_length resolved session_id subject virus mailer	MSISDN}`	Sets what columns will appear when the selected log type is viewed in the web-based manager. The keyword, `MSISDN`, is available only when the command `set log msisdn` is enabled.	No default

History

FortiMail v2.8	New.
FortiMail v3.0 MR3	Added `MSISDN` keyword.

Related topics

- set log msisdn
- set log setting local
- set log setting syslog
- set log policy destination event
- set log policy destination spam
- set log policy destination virus
- set log policy destination history

log view loglevel

Use this command to configure the log severity level of what displays when viewing log messages in the web-based manager.

Syntax

To set the log severity level that will display in the web-based manager

```
set log view loglevel {event | history | spam | virus} loglevel
  <severity_integer>
```

Keywords/Variables	Description	Default
`loglevel {event | history | spam | virus}`	Sets the log type	No default
`loglevel <severity_integer>`	Sets the destination log severity level. Use the ? to list the following log levels: 0=Emergency 1=Alert 2=Critical 3=Error 4=Warning 5=Notification 6=Information Logs will include items of the level you set and higher. Set level to 6 if you want to include all log severity levels.	No default

History

FortiMail v2.8	New.

Related topics

- set log setting localset
- set log setting syslog
- set log policy destination event
- set log policy destination spam
- set log policy destination virus
- set log policy destination history

mailserver access

Use this command to configure, delete, and reorder mailserver access rules.

Access rules are processed in numerical order. Use the 'move' keyword to change the order of rules to achieve your desired processing order. If there are two rules that apply, the rule with the lowest number will be processed first.

Syntax

```
set mailserver access rule <number> set sender_pattern <pattern_str>
  {yes | no} recipient_pattern <pattern_str> {yes | no} ip_mask
  <ipv4_addr>/<netmask> reverse_dns_pattern <pattern_str> {yes | no}
  authenticated {yes | no} tlsprofile <profile_str> action
  {relay | bypass | reject | discard}

  set mailserver access rule <number> move <to>

  set mailserver access rule <number> delete
```

Keywords and Variables	Description	Default
`rule <number>`	Enter the number for this rule. Numbers are used for processing order of the rules, lowest numbers first.	
`{set | move | delete}`	Select one of `set`, `move`, or `delete` to change mailserver access. • set - Select to configure an access rule. • move - Select to change when this rule is processed. • delete - Select to remove a rule from the list	
`sender_pattern <pattern_str>`	A complete or partial sender address to match for this rule.	
`{yes | no}`	Select `yes` to use regular expression syntax as part of the pattern.	
`recipient_pattern <pattern_str>`	A complete or partial sender address to match for this rule.	
`ip_mask <ipv4_addr>/ <netmask>`	Enter the IP address and netmask of the sender.	
`reverse_dns_pattern <pattern_str>`	A complete or partial DNS entry match for this rule.	
`authenticated {yes | no}`	Enter yet to have the rule match only authenticated sessions. Enter yes to have the rule apply to both authenticated and unauthenticated sessions.	

Keywords and Variables	Description	Default
`tlsprofile <profile_str>`	To enforce TLS connection attributes, select a TLD profile.	
`permission {ok | relay | reject | discard}`	Select the level of permission for this domain: • `relay` - the FortiMail unit allows matching messages after normal processing. • `bypass` - the FortiMail unit allows matching messages after all normal processing except antispam scans. The antispam scans are not performed. • `reject` - the FortiMail unit rejects email matching this rule. • `discard` - the FortiMail unit discards email matching this rule. The response that the FortiMail unit sends differs for reject and discard. For reject, a reject response is sent to the server or client attempting to send the email message. For discard, the FortiMail unit does not send a response to the server or client attempting to send the email message.	

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Major change to command. Added `set, move, delete, rule, sender_pattern, recipient_pattern, reverse_dns_pattern, and ip_mask` keywords.
FortiMail v3.0 MR4	Added `authenticated` and `tlsprofile`.

mailserver archive account

Use this command to configure the archive account settings.

Syntax

```
set mailserver archive account <account_str>
set mailserver archive account <account_str> forward <email_str>
set mailserver archive account <account_str> password <pwd_str>
set mailserver archive account <account_str> quotafull {overwrite |
  noarchive}
set mailserver archive account <account_str> rotatesize <size_int>
set mailserver archive account <account_str> rotatetime <time_int>
set mailserver archive account <account_str> status {enable | disable}
```

Keywords and Variables	Description	Default
`<account_str>`	Enter the email archiving account name.	`archive`
`forward <email_str>`	Enter the email address to which all archived messages will also be forwarded. If no address is entered, forwarding will not occur. If an email address is entered to enable forwarding, previously archived mail will not be forwarded.	No default.
`password <pwd_str>`	Enter the email archiving account password.	No default.
`quotafull {overwrite | noarchive}`	Select the action taken with new log entries when the disk space quota is reached. • `{overwrite}` to overwrite the oldest mailbox when the quota is reached. • `{noarchive}` to stop archiving when the quota is reached.	`overwrite`
`rotatesize <size_int>`	Enter the size, in megabytes, at which the email archiving mailbox will be rotated. • `<size_int>` is the email archiving mailbox rotation size in megabytes. The allowed range is from 10 to 200.	`100`
`rotatetime <time_int>`	Enter the email archiving mailbox rotation time, in days. • `<size_int>` is the increment after which the archive mailbox is rotated. The allowed range is from 1 to 365 days.	`7`
`status {enable | disable}`	Enable or disable email archiving.	`disable`

History

FortiMail v3.0 New.

Related topics

- set mailserver archive exemptlist
- set mailserver archive local quota
- set mailserver archive policy
- set mailserver archive remote

mailserver archive exemptlist

Use this command to configure the exemptlist and exemptlist entries.

Syntax

```
set mailserver archive exemptlist exemptid <id_int> content <content_str>
set mailserver archive exemptlist exemptid <exemptid_str> status {enable
   | disable}
set mailserver archive exemptlist exemptid <exemptid_str> type {sender |
   recipient | spam}
set mailserver archive exemptlist move <position_int> to <new_int>
```

Keywords and Variables	Description	Default
`<id_int>`	Enter the ID number of the exemption item.	
`<content_str>`	Enter the text to be searched for. Wildcards are acceptable. If the policy type is "Spam", `<content_str>` is ignored.	
`status {enable | disable}`	Enable or disable the specified exemptlist entry.	`disable`
`type {sender | recipient | spam}`	Enter the exemptlist entry type. • `{sender}` The sender field of each email message will be searched for the text specified with the content command. • `{recipient}` The recipient field of each email message will be searched for the text specified with the content command. • `{spam}` Messages detected as spam by the FortiMail unit will match this entry type. Any text specified with the content command is ignored.	`sender`
`move <position_int> to <new_int>`	Changes the position of an exempt item in the list. • `<position_int>` is the current list position of the exempt list policy to be moved. • `<new_int>` is the destination list position number.	

To view the existing entries in the archive exempt list, enter this command:

```
set mailserver archive exemptlist exemptid ?
```

History

FortiMail v3.0 New.

Related topics

- set mailserver archive account
- set mailserver archive local quota
- set mailserver archive policy
- set mailserver archive remote

mailserver archive local quota

Use this command to specify the archive quota if the archive is stored on the FortiMail unit.

Syntax

```
set mailserver archive local quota <quota_int>
```

Keywords and Variables	Description	Default
`quota <quota_int>`	Enter the local disk quota for archived email. The quota is specified in gigabytes. The acceptable range of values depends on the amount of free disk space.	1

History

FortiMail v3.0	New.

Related topics

- set mailserver archive account
- set mailserver archive exemptlist
- set mailserver archive policy
- set mailserver archive remote

mailserver archive policy

Use this command to configure archive policies.

Syntax

```
set mailserver archive policy move <position_int> to <new_int>
set mailserver archive policy policyid <policyid_int> content
  <content_str>
set mailserver archive policy policyid <policyid_int> status {enable |
  disable}
set mailserver archive policy policyid <policyid_int> type {sender |
  recipient | subject | body | attachment-name}
```

Keywords and Variables	Description	Default
`<id_int>`	Enter the ID number of the archive policy.	
`move <position_int> to <new_int>`	Changes the position of an archive policy in the list. • `<position_int>` is the current list position of the archive policy to be moved. • `<new_int>` is the destination list position number.	
`<content_str>`	Enter the text to be searched for. Wildcards are acceptable if the type is Sender, Recipient, or Attachment-name.	
`status {enable | disable}`	Enable or disable the specified archive policy.	`enable`
`type {sender | recipient | subject | body | attachment-name}`	Enter the archive policy type. • `{sender}` The sender field of each email message will be searched for the text specified with the content command. • `{recipient}` The recipient field of each email message will be searched for the text specified with the content command. • `{subject}` Messages detected as spam by the FortiMail unit will match this entry type. Any text specified with the content command is ignored. • `{body}` The body of each email message will be searched for the text specified with the content command. • `{attachment-name}` The name of any attached files are examined for the text specified with the content command.	`sender`

To view the existing entries in the archive policy list, enter this command:

```
set mailserver archive policy policyid ?
```

History

FortiMail v3.0 New.

Related topics

- set mailserver archive account
- set mailserver archive exemptlist
- set mailserver archive local quota
- set mailserver archive remote

mailserver archive remote

Use this command to specify the settings used when the FortiMail unit will store its email archive on a remote host.

Syntax

```
set mailserver archive remote directory <directory_str> ip <host_ipv4>
  localquota <quota_int> password <pwd_str> protocol {FTP | SFTP}
  remotequota <quota_int> username <usr_str>
```

Keywords and Variables	Description	Default
`directory <dir_str>`	Enter the directory on the remote host to be used for archiving email.	
`ip <host_ipv4>`	Enter the IP of the remote host to be used for archiving email.	
`localquota <quota_int>`	Enter the FortiMail unit cache quota. Email archived on a remote host is also cached by the FortiMail unit. The local quota amount is specified in gigabytes. The available range depends on the amount of free disk space.	`1`
`password <pwd_str>`	Enter the password for logging in to the remote host.	
`protocol {FTP | SFTP}`	Choose the communication protocol the FortiMail unit will use when sending data to the remote host.	`SFTP`
`remotequota <quota_int>`	Enter the disk quota for the remote host to archive email. The remote quota amount is specified in gigabytes. Enter 0 to specify no limit.	`0`
`username <usr_str>`	Enter the user name for logging in to the remote host.	

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Capitalized variables for `protocol` keyword.

Related topics

- set mailserver archive account
- set mailserver archive exemptlist
- set mailserver archive local quota
- set mailserver archive policy

mailserver deadmail

Use this command to enter the number of days to keep email with incorrect recipient and sender addresses.

Syntax

```
set mailserver deadmail <value>
```

`<value>` is the time in days - from 1 to 365.

History

FortiMail v3.0	New.

mailserver portnumber

Use this command to enter email port numbers for the FortiMail unit.

Syntax

```
set mailserver portnumber pop3 <port_number> (server mode)
set mailserver portnumber smtp <port_number>
set mailserver portnumber smtps <port_number>
```

Keywords and Variables	Description	Default
`pop3 <port_number>`	Enter the POP3 server port number for the FortiMail unit. This command is only available in server mode.	`110`
`smtp <port_number>`	Enter the SMTP server port number for the FortiMail unit.	`25`
`smtps <port_number>`	Enter the SMTPS server port number for the FortiMail unit.	`465`

History

FortiMail v3.0	New.

mailserver proxy smtp interface

Use this command to configure SMTP proxy behavior on an interface. The unknown keyword is for handling unknown servers.

Syntax

```
set mailserver proxy smtp interface <port> imode {pass-through | drop |
  proxy} omode {pass-through | drop | proxy} local {enable | disable}
```

Keywords and Variables	Description	Default
`interface <port>`	Enter the interface where the proxy behavior is being configured.	No default.
`imode {pass-through	drop	proxy}`	Select one of the following behaviors for incoming traffic: • pass-through - bridge the traffic • drop - drop the traffic • proxy - proxy the traffic.	
`omode {pass-through	drop	proxy}`	Select one of the following behaviors for outgoing traffic: • pass-through - bridge the traffic • drop - drop the traffic proxy - proxy the traffic	
`local {enable	disable}`	Select enable to allow access to the local SMTP server on this interface.	

History

FortiMail v3.0 New.

Related topics

- set mailserver proxy smtp unknown

mailserver proxy smtp unknown

Use this command to configure SMTP proxy behavior for unknown servers.

Syntax

To change general unknown server settings:

```
set mailserver proxy smtp unknown <hide> <original>
```

The proxy SMTP unknown options are also available on a per domain basis under “policy modify tp” on page 295.

Keywords and Variables	Description	Default
`<hide>`	Select “yes” to hide the transparent unit or “no” for it to be visible. This option determines if the header is forwarded untouched by the FortiMail unit (yes) or if the FortiMail unit visibly processes the mail headers (no).	No default.
`<original>`	Select “yes” to use the default domain mail server or “no” to relay the mail through the FortiMail unit by default.	

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Removed `mx, server, client,` and `tp` keywords.

Related topics

- set mailserver proxy smtp interface

mailserver relayserver

Use this command to configure the relay server settings including name, port, and authentication.

Syntax

```
set mailserver relayserver <name_str> port <port_number>
  authentication {enable | disable} username <name_str>
  password <pwd_str> type <auth_type>
```

Keywords and Variables	Description	Default
`<name_str>`	Enter the FQDN name of the relay server.	No default.
`port <port_number>`	Enter the port number to use when communicating with this relay server.	
`authentication {enable | disable}`	Select `enable` to turn on authentication for the relay server.	
`username <name_str>`	Enter the username for the account on the relay server to be used for authentication purposes.	
`password <pwd_str>`	Enter the password for the account on the relay server to be used for authentication purposes.	
`type <auth_type>`	Select one of the types of authentication for the relay server: • AUTO • PLAIN • LOGIN • DIGEST-MD5 • CRAM-MD5	`auto`

History

FortiMail v3.0 New.

mailserver smtp deferbigmsg

Use this command to configure the period when deferred oversized emails will start and stop being processed. Deferring oversized emails can offload processing to a time of day when email traffic is not as busy.

Syntax

```
set mailserver smtp deferbigmsg starttime <hh:mm>
set mailserver smtp deferbigmsg stoptime <hh:mm>
```

Keywords and Variables	Description	Default
`starttime <hh:mm>`	Enter the time that oversized email will start being processed. Time is in 24 hour format.	No default.
`stoptime <hh:mm>`	Enter the time that oversized email will stop being processed. Time is in 24 hour format.	No default.

History

FortiMail v3.0	New.

mailserver smtp delivery

Selecting ‘yes’ for this command will turn off ESMTP delivery.

Syntax

```
set mailserver smtp delivery noesmtp {yes | no}
```

History

FortiMail v3.0 MR3 New.

mailserver smtp dsn_

Use this command to configure the delivery status notification (DSN) messages sender information.

Syntax

```
set mailserver smtp dsn_displayname <name_str>
set mailserver smtp dsn_sender <email_str>
```

`<name_str>` is the sender’s name the notification is from. An example would be postmaster.

`<email_str>` is the sender’s email address the notification is sent from. An example for the domain example.com would be postmaster@example.com.

History

FortiMail v3.0	New.

mailserver smtp ldap_domain_check

Use this command to check the validity of domains not configured on the FortiMail unit with LDAP verification. Email messages to domains passing this check can be routed to internal mail servers using LDAP routing.

Syntax

```
set mailserver smtp ldap_domain_check <enable | disable> ldap_profile
  <profile_str> auto_associate <enable|disable> internal_domain
  <domain_str>
```

Keywords and Variables	Description	Default
`ldap_domain_check <enable | disable>`	When enabled, the FortiMail unit will use LDAP verification to check the validity of domains not configured on the FortiMail unit. Email messages to domains passing this check can be routed to internal mail servers using LDAP routing.	`disable`
`ldap_profile <profile_str>`	Enter the LDAP profile to use for domain verification.	
`auto_associate <enable|disable>`	When enabled, domains passing LDAP verification will be automatically created as domain associations.	`disable`
`internal_domain <domain_str>`	Enter the domain the automatically created domain associations will be a part of.	

History

FortiMail v3.0 MR4 New.

mailserver smtp queue

Use this command to configure the time outs and retries for undelivered mail in queues.

Note: The units of time are not the same for all keywords in this command.

Syntax

```
set mailserver smtp queue dsn_timeout <dsn_timeout> retry <retry
  interval> timeout <timeout> warning <warning time>
```

Keywords and Variables	Description	Default
`dsn_timeout <dsn_timeout>`	Select the maximum number of days a delivery status notification (DSN) message can remain in the mail queues. The valid range is from zero to ten days. After the maximum time has been reached, the DSN email will be returned as undeliverable. If the maximum time is set to zero days, delivery will be attempted one time and then the DSN email will be returned as undeliverable.	5 days
`retry <retry interval>`	Select the number of minutes between delivery retries for queues. The valid range is from 10 to 120 minutes. Adjusting this value lower will help deliver messages faster.	27 minutes
`timeout <timeout>`	Select the maximum number of days an email can remain in a mail queue. The valid range is from one to ten days. After the maximum time has been reached, the email will be returned as undeliverable.	5 days
`warning <warning time>`	Select the number of hours before a warning is sent to the sender notifying them the message has been deferred. The valid range is from 1 to 24 hours.	4 hours

History

FortiMail v3.0 MR2 New.

mailserver smtpauth

Use this command to enable or disable authentication using SMTP, SMTP over TLS, or SMTPS.

If authentication is not configured, clients can still attempt to authenticate, though they will always fail. Using this command to disable the client's ability to authenticate will prevent this situation from occurring.

Syntax

```
set mailserver smtpauth smtp {enabled | disabled}
set mailserver smtpauth smtpovertls {enabled | disabled}
set mailserver smtpauth smtps {enabled | disabled}
```

History

FortiMail v3.0	New.
FortiMail v3.0 MR4	Added the `smtp`, `smtpovertld`, and `smtps` options.

mailserver smtpssl

Use this command for SMTP over secure socket layer (SSL).

Syntax

```
set mailserver smtpssl {enabled | disabled}
```

History

FortiMail v3.0 MR3 New.

mailserver smtp storage

Use this command to configure local or network file storage (NFS) options.

Syntax

```
set mailserver smtp storage local

set mailserver smtp storage nfs dir <nfs_server_dir>
set mailserver smtp storage nfs ip <ipv4_addr>
```

Keywords and Variables	Description	Default
`local | nfs`	Select the type of storage for the FortiMail unit. • local - use local storage • nfs - use NFS	N/A
`type {disable | client | <type>}`	Select the type of storage to be used in a central quarantine configuration. • disable - • client - This unit connects as a client to a central quarantine server. • server - This unit is a central quarantine server. Option available only for high-end model FortiMail units	disable
`dir`	Select the directory to use on the NFS storage.	
`ip`	Select the IP address of the NFS storage.	

History

FortiMail v3.0 MR3 New.

mailserver smtp storage cquar

Use this command to configure central quarantine mail storage options.

Central quarantine stores quarantined email on a separate high-end model FortiMail unit. This reduces the resources required on the local unit.

The `allowance` keyword is only available when the FortiMail unit is a central quarantine server.

The `remoteserver` keyword is only available for FortiMail client units.

Syntax

```
set mailserver smtp storage cquar type {disable | client | server}

set mailserver smtp storage cquar allowance add name <name_str> ip
  <ipv4_addr>

set mailserver smtp storage cquar allowance change name <name_str> ip
  <ipv4_addr>

set mailserver smtp storage cquar allowance remove name <name_str>

set mailserver smtp storage cquar remoteserver name <name_str> host
  <ipv4_addr>
```

Keywords and Variables	Description	Default
`type {disable | client | server}`	Select the type of storage to be used in a central quarantine configuration as one of: • disable - central quarantine is not used on this unit. • client - This unit connects as a client to a central quarantine server. • server - This unit is a central quarantine server. Option available only for high-end model FortiMail units	disable
`add | change | remove`	Select the action to perform	
`name <name_str>`	Enter the name of the FortiMail client unit.	
`ip <ipv4_addr>`	Enter the IP address of the FortiMail client unit.	
`remoteserver`		

Example

This example will configure a FortiMail unit as a server, and will add “FortiMailClient1” and FortiMailClient2” as quarantine clients that will connect to this server.

```
set mailserver smtp storage cquar type server
set mailserver smtp storage cquar allowance add name FortiMailClient1 ip
  10.10.10.10
set mailserver smtp storage cquar allowance add name FortiMailClient2 ip
  10.10.20.10
```

This example will configure a FortiMail unit as a client with the name “`FortiMailClient1`” that will connect to a central quarantine server at IP address `10.10.10.2`. After being configured as a client, the FortiMail unit will not store any quarantined messages locally.

```
set mailserver smtp storage cquar type client
set mailserver smtp storage cquar remoteserver name “FortiMailClient1”
  host 10.10.10.2
```

History

FortiMail v3.0 MR3 New.

mailserver systemquarantine

Use this command to configure the system quarantine settings.

Syntax

```
set mailserver systemquarantine account <name_str> password <pwd_str>
set mailserver systemquarantine forward <address_str>
set mailserver systemquarantine quota <quota_int>
set mailserver systemquarantine quotafull {overwrite | noquarantine}
set mailserver systemquarantine rotatesize <size_int> rotatetime
  <time_int>
```

Keywords and Variables	Description	Default

`account <name_str>`
`password <pwd_str>`
	Enter the user ID and password for the system quarantine admin account.	User ID:
		`systemquarantine`
		Password:
		`systemquarantine`

`forward <address_str>`	Enter an email address to which all messages diverted to the system quarantine will be copied.	
`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.	`1`
`quotafull {overwrite | noquarantine}`	Enter the action the FortiMail unit should take when the system quarantine reaches its quota size. • `overwrite -` will have a new message replace the oldest in the system quarantine. • `noquarantine -` will prevent any new messages from being quarantined. Note however that `noquarantine` will still prevent messages from being delivered. Since they're not quarantined, they're simply deleted.	`overwrite`

`rotatesize <size_int>`
`rotatetime <time_int>`
	Configures the size and time thresholds which trigger system quarantine rotation. When the mailbox reaches the rotation size or time threshold, whichever occurs first, the mailbox (mbox file) will be renamed and backed up. A new mailbox file will be generated, into which the new email is saved.
	• `<size_int>` is the rotation size, from 10 to 200 megabytes.
	• `<time_int>` is the rotation time, from 1 to 365 days.
		rotation size: 100
		rotation time: 7

History

FortiMail v3.0 New.

Related topics

- set content modify action
- set content modify monitor action

misc profile delete

Use this command to delete a misc profile. This command is available in server mode only.

Syntax

```
set misc profile <name_str> delete
```

`<name_str>` is the name of the misc profile.

History

FortiMail v3.0	New.

Related topics

- set misc profile rename-to

misc profile modify quota

Use this command to change the disk space quota in megabytes for the mail user account, or accounts, for the specified profile. This command is available in server mode only.

Syntax

```
set misc profile <name_str> modify quota <quota_int>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the misc profile.	
`<quota_int>`	Enter the per-user disk space quota in megabytes. The acceptable range is from 0 to 4000, where 0 is unlimited.	`0`

History

FortiMail v3.0	New.

Related topics

- set misc profile modify userstatus
- set misc profile modify webmailaccess

misc profile modify userstatus

Use this command to enable or disable the user account, or accounts, for the specified profile. This command is available in server mode only.

Syntax

```
set misc profile <name_str> modify userstatus {enable | disable}
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the misc profile.	
`userstatus {enable | disable}`	Enables or disable the user account, or accounts, for the specified profile. When disabled, the user will not be able to log in to the webmail interface or send mail with a mail client. Any mail sent to the user will be rejected with a “user unknown” message.	`disable`

History

FortiMail v3.0 New.

Related topics

- set misc profile modify quota
- set misc profile modify webmailaccess

misc profile modify webmailaccess

Enables or disables Webmail access for the specified profile. This command is available in server mode only.

Syntax

```
set misc profile <name_str> modify webmailaccess {enable | disable}
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the misc profile.	
`webmailaccess {enable | disable}`	Enables or disable the ability of the user to log in to the webmail interface. When disabled, the user will be able to enter their email address and password, but a 'Login Incorrect!' error will be displayed.	`disable`

History

FortiMail v3.0	New.

Related topics

- set misc profile modify quota
- set misc profile modify userstatus

misc profile rename-to

Use this command to rename a misc profile. This command is available in server mode only.

Syntax

```
set misc profile <name_str> rename-to <new_str>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the misc profile.	
`<new_str>`	Enter the new name of the misc profile.	

History

FortiMail v3.0 New.

Related topics

- set misc profile delete

out_content delete

Use this command to delete a outgoing content profile.

Syntax

```
set out_content <name_str> delete
```

`<name_str>` is the name of the outgoing content profile.

History

FortiMail v3.0	New.

Related topics

- set out_content modify filetype
- set out_content modify monitor

out_content modify action

Use this command to select the action to be taken with messages matching the specified outgoing content profile.

Syntax

```
set out_content <name_str> modify action {treat_as_spam | reject| discard
   | replace | quarantine | forward} [forwardaddr <addr_str>]
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the outgoing content profile.	
`action {discard	forward	reject	replace	treat_as_spam}`	Select the action to be taken on messages matching the active outgoing content profile. • `{discard}` deletes the message. • `{forward}` sends the message to the specified email address instead of the recipient. • `{reject}` causes the FortiMail unit to not accept delivery of the infected message. An error is returned to the system attempting delivery. • `{replace}` strips the infected attachment and replaces it with a custom message. • `{treat_as_spam}` handles the infected message according to the action set in the applicable antispam profile.	`replace`
`forwardaddr <addr_str>`	Enter the email address to be used if the selected action is forward. When forward is selected as the action, matching messages are forwarded to the specified email address.	

History

FortiMail v3.0 New.

Related topics

- set out_content modify action
- set out_content modify monitor

out_content modify bypass_on_auth

Use this command to allow messages to bypass the outgoing content filters if SMTP authorization is enabled and the delivering system successfully authenticates.

Syntax

```
set out_content <name_str> modify bypass_on_auth {enable | disable}
```

`<name_str>` is the name of the outgoing content profile.

History

FortiMail v3.0	New.

Related topics

- set out_content modify action
- set out_content modify filetype

out_content modify filetype

Use this command to block email attachments that match the specified file type.

Syntax

```
set out_content <name_str> modify filetype <filetype_str> {blocked |
  not-blocked}
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the outgoing content profile.	
`<filetype_str>`	Select the file type. Valid types are • `video` • `audio` • `image` • `application/executable` • `application/document` • `application/archive` • `application/other` This option includes all file types not specified by the other listed types.	
`{blocked | not-blocked}`	Select `blocked` to trigger the content action against messages containing the specified type of file attachment. Select `not-blocked` to allow the specified type of file attachment.	`not-blocked`

History

FortiMail v3.0 New.

Related topics

- set out_content modify action
- set out_content modify monitor

out_content modify monitor action

Use this command to select the action to be taken with messages matching the specified outgoing content monitor profile.

Syntax

```
set out_content <name_str> modify monitor <profile_int> action {none |
  discard | forward | quarantine | reject | replace | review |
  treat_as_spam}
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the outgoing content profile.	
`<profile_int>`	Enter the outgoing content monitor profile number.	
`action {none	discard	forward	reject	replace	review	treat_as_spam}`	Select the action to be taken with messages matching the specified outgoing content monitor profile. • `{none}` no action is taken, though subject and/or header tagging occurs if enabled. • `{discard}` deletes the message. • `{forward}` sends the message to the specified email address instead of the recipient. • `{reject}` causes the FortiMail unit to not accept delivery of the infected message. An error is returned to the system attempting delivery. • `{replace}` strips the infected attachment and replaces it with a custom message. • `{review}` stops messages matching the monitor profile and places them into the system quarantine. These messages are not included in the spam report sent to users. Rather, an administrator must release or delete these messages after reviewing them. • `{treat_as_spam}` handles the infected message according to the action set in the applicable antispam profile.	`none`

History

FortiMail v3.0 New.

Related topics

- set out_content modify monitor

out_content modify monitor

Use this command to configure outgoing content monitor profiles.

Syntax

```
set out_content <name_str> modify monitor <profile_int> delete
set out_content <name_str> modify monitor <profile_int> dict_profile
  <dict_int>
set out_content <name_str> modify monitor <profile_int> {enable |
  disable}
set out_content <name_str> modify monitor <profile_int> moveto <new_int>
set out_content <name_str> modify monitor <profile_int> tags header
  {enable | disable}
set out_content <name_str> modify monitor <profile_int> tags htag
  <tag_str>
set out_content <name_str> modify monitor <profile_int> tags stag
  <tag_str>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the outgoing content profile.	
`<profile_int>`	Enter the outgoing content monitor profile number.	
`<dict_int>`	Enter the dictionary profile ID number to use for the specified outgoing content monitor profile.	
`{enable | disable}`	Enable or disable the specified outgoing content monitor profile.	`enable`
`moveto <new_int>`	Moves the specified outgoing content monitor profile to a new position in the list. • `<new_int>` is the destination content profile number.	
`tags header {enable | disable}`	Enable or disable the labeling of matching messages by adding a tag to the header.	`disable`
`tags htag <tag_str>`	Enter the text to be used as the tag when header tagging is enabled.	
`tags subject {enable | disable}`	Enable or disable the labeling of matching messages by adding a tag to the subject.	`disable`
`tags stag <tag_str>`	Enter the text to be used as the tag when subject tagging is enabled.	

History

FortiMail v3.0	New.

Related topics

- set out_content modify monitor action

out_policy profile delete

Use this command to delete an outgoing recipient-based policy. This command applies to gateway and transparent modes only.

Syntax

```
set out_policy <user_str> delete
```

`<user_str>` is the user the policy applies to.

History

FortiMail v3.0	New.

Related topics

- set out_policy move-to
- set out_policy rename-to

out_policy modify

Use these commands to configure outgoing recipient-based policies. This command applies to gateway and transparent modes only.

Syntax

```
set out_policy <user_str> modify as <name_str>
set out_policy <user_str> modify av <name_str>
set out_policy <user_str> modify content <name_str>
```

Keywords and Variables	Description	Default
`<user_str>`	Enter the outgoing recipient-based policy user ID.	
`modify as <name_str>`	Select the antispam profile to apply to the selected recipient-based policy.	`antispam_out_def`
`modify av <name_str>`	Select the antivirus profile to apply to the selected recipient-based policy.	`antivirus_def`
`modify content <name_str>`	Select the content profile to apply to the selected recipient-based policy.	`content_out_def`

History

FortiMail v3.0 New.

Related topics

- set out_policy profile delete
- set out_policy move-to
- set out_policy rename-to

out_policy move-to

Use this command to move an outgoing recipient-based policy to a new position in the policy list. This command applies to gateway and transparent modes only.

Syntax

```
set out_policy <user_str> move-to <new_int>
```

Keywords and variables	Description	Default
`<user_str>`	Enter the outgoing recipient-based policy user ID.	
`move-to <new_int>`	Enter the new position the policy will occupy.	

History

FortiMail v3.0	New.

Related topics

- set out_policy profile delete
- set out_policy rename-to

out_policy rename-to

Use this command to rename an outgoing recipient-based policy. This command applies to gateway and transparent modes only.

Syntax

```
set out_policy <user_str> rename-to <new_str>
```

Keywords and variables	Description	Default
`<user_str>`	Enter the outgoing recipient-based policy user ID.	
`rename-to <new_str>`	Enter the new user ID.	

History

FortiMail v3.0	New.

Related topics

- set out_policy profile delete
- set out_policy move-to

out_profile profile delete

Use this command to delete an outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> delete
```

`<name_str>` is the name of the outgoing antispam profile.

History

FortiMail v3.0	New.

Related topics

- set out_profile profile rename-to

out_profile profile modify actions

Use these command to modify the actions of an outgoing antispam profile.

Reject, discard, and forward are mutually exclusive. No more than one can be enabled at any time. If the specified profile does not exist, it is created.

Syntax

```
set out_profile profile <name_str> modify actions discard {enable |
  disable}
set out_profile profile <name_str> modify actions emailaddr <address_str>
set out_profile profile <name_str> modify actions forward {enable |
  disable}
set out_profile profile <name_str> modify actions reject {enable |
  disable}
set out_profile profile <name_str> modify actions review {enable |
  disable}
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the outgoing antispam profile.	
`discard {enable | disable}`	Enable or disable discarding spam without sending reject responses to the senders.	`disable`
`emailaddr <address_str>`	Enter the email address to which messages are forwarded when forwarding is enabled.	No default
`forward {enable | disable}`	Enable or disable forwarding of spam messages.	`disable`
`reject {enable | disable}`	Enable or disable the FortiMail unit to reject spam and send reject responses to the sending system.	`disable`
`review {enable | disable}`	Enable or disable the redirection of outbound spam to the system quarantine. If enabled, the messages detected as spam must be released or deleted by an administrator. These messages will not appear on the spam summary.	`disable`

History

FortiMail v3.0	New.
FortiMail v3.0 MR1	Keyword `summary` removed.

Related topics

- set out_profile profile modify individualaction scanner
- set out_profile profile modify scanoptions

out_profile profile modify bannedword

Use this command to enable or disable outgoing banned word filtering for the specified profile.

Syntax

```
set out_profile profile <name_str> modify bannedword {enable | disable}
```

`<name_str>` is the name of the profile. By default, banned word scanning is disabled.

History

FortiMail v3.0	New.

Related topics

- set out_profile profile modify bannedwordlist
- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify bannedwordlist

Use these command to modify the banned word list for an outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify bannedwordlist <word_str> add
set out_profile profile <name_str> modify bannedwordlist <word_str>
  delete
set out_profile profile <name_str> modify bannedwordlist <word_str>
  move-to <position_int>
set out_profile profile <name_str> modify bannedwordlist <word_str>
  rename-to <new_str>
```

Keywords and variables	Description
`<name_str>`	Enter the name of the outgoing antispam profile to modify.
`<word_str>`	The word entry you want to modify in the profile's banned word list.
`add`	Add the new banned word.
`delete`	Delete the banned word.
`move-to <position_int>`	Change the position of the word in the banned word list. Each word is numbered, the first is 1, the second 2, and so on. • `<position_int>` is the word's new position.
`rename-to <new_str>`	Change the word entry.

History

FortiMail v3.0 New.

Related topics

- set out_profile profile modify bannedword
- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify bayesian

Use this command to enable or disable Bayesian spam filtering for the specified antispam profile.

Syntax

```
set out_profile profile <name_str> modify bayesian {enable | disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`{enable | disable}`	Enable or disable Bayesian filtering for the specified outgoing antispam profile.	`disable`

History

FortiMail v3.0 New.

Related topics

- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify deepheader

Use this command to enable or disable deep header scanning or for the specified profile. The two separate checks that make up the deep header scan can also be individually enabled or disabled.

Syntax

```
set out_profile profile <name_str> modify deepheader scanner
  {enable | disable}
set out_profile as profile <name_str> modify deepheader checkip
  {enable | disable}
set out_profile as profile <name_str> modify deepheader headeranalysis
  {enable | disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`scanner {enable | disable}`	Enable or disable the deep header scan for the specified profile.	`disable`
`checkip {enable | disable}`	Enable or disable the black IP portion of the deep header scan for the specified profile.	`disable`
`headeranalysis {enable | disable}`	Enable or disable the headers analysis portion of the deep header scan for the specified profile.	`disable`

History

FortiMail v3.0	New.
FortiMail v3.0 MR1	`checkip` and `headeranalysis` added.

Related topics

- set as profile modify actions
- set as profile modify deepheader
- set as profile modify individualaction scanner
- set out_profile profile modify deepheader
- get spam deepheader

out_profile profile modify dictionary

Use these commands to configure dictionary scans for the specified outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify dictionary dict_profile
  <dict_int>
set out_profile profile <name_str> modify dictionary scanner {enable |
  disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`dict_profile <dict_int>`	Select the dictionary profile to be used for dictionary scans. • `<dict_int>` is the dictionary profile number.	
`scanner {enable | disable}`	Enable or disable dictionary scanning for the specified profile.	`disable`

History

FortiMail v3.0 New.

Related topics

- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify dnsbl

Use this command to enable or disable communication with the DNSBL servers to scan email for the specified outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify dnsbl {enable | disable}
```

`<name_str>` is the name of the profile. By default, the DNSBL lookup is disabled.

History

FortiMail v3.0	New.

Related topics

- set out_profile profile modify dnsblserver
- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify dnsblserver

Use these commands to modify the DNSBL server list for an outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify dnsblserver <host_str> add
set out_profile profile <name_str> modify dnsblserver <host_str> delete
set out_profile profile <name_str> modify dnsblserver <host_str> move-to
  <new_int>
set out_profile profile <name_str> modify dnsblserver <host_str>
  rename-to <new_str>
```

Keywords and variables	Description
`<name_str>`	Enter the name of the antispam profile to modify.
`<host_str>`	The DNSBL server entry you want to modify in the profile.
`add`	Add the new DNSBL server.
`delete`	Delete the DNSBL server.
`move-to <new_int>`	Change the position of the DNSBL server in the server list. Each entry is numbered, the first is 1, the second 2, and so on. • `<new_int>` is the entry’s new position.
`rename-to <new_str>`	Change the DNSBL server hostname.

History

FortiMail v3.0 New.

Related topics

- set out_profile profile modify dnsbl
- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify fortishield

Use these commands to configure FortiGuard-Antispam functions for an outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify fortishield checkip {enable |
  disable}
set out_profile profile <name_str> modify fortishield scanner {enable |
  disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`checkip {enable | disable}`	Enable or disable FortiGuard-Antispam IP address checking for the specified profile.	`disable`
`scanner {enable | disable}`	Enable or disable FortiGuard-Antispam scanning for the specified profile.	`disable`

History

FortiMail v3.0	New.

Related topics

- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify greylist

Use this command to enable or disable greylisting for an outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify greylist {enable | disable}
```

`<name_str>` is the name of the profile. By default, greylisting is disabled.

History

FortiMail v3.0	New.

Related topics

- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify heuristic

Use these commands to configure heuristic scanning for an outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify heuristic lower-level
  <lower_int>
set out_profile profile <name_str> modify heuristic scanner {enable |
  disable}
set out_profile profile <name_str> modify heuristic upper-level
  <upper_int>
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`lower-level <lower_int>`	Enter the lower level threshold for heuristic scanning for the specified profile.	`-20.000000`
`scanner {enable | disable}`	Enable or disable heuristic scanning for the specified profile.	`disable`
`upper-level <upper_int>`	Enter the upper level threshold for heuristic scanning for the specified profile.	`10.000000`

History

FortiMail v3.0 New.

Related topics

- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify imagespam

Use these commands to configure an outgoing antispam profile to identify spam messages in which the text is stored as an embedded graphics file.

Syntax

```
set out_profile profile <name_str> modify imagespam aggressive {enable |
   disable}
set out_profile profile <name_str> modify imagespam scanner {enable |
   disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`aggressive {enable | disable}`	Enable or disable more intensive examination of email messages containing images. This option will also force the examination of image file attachments in addition to embedded images. The additional scanning workload could affect performance with traffic containing image files.	`disable`
`scanner {enable | disable}`	Enable or disable scanning of email for image-based spam messages.	`disable`

History

FortiMail v3.0	New.

Related topics

- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify individualaction scanner

Use these commands to set the action each spam detection method takes for messages detected as spam.

Syntax

```
set out_profile profile <name_str> modify individualaction scanner
  {bannedword | bayesian | deepheader | dictionary | dnsbl | fortishield
  | heuristic | imagespam | surbl | virus} action {default | discard |
  forward | reject | review | subject}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`scanner`	Select the spam detection method.	no default
`action`	Select the action to take. • Set `default` to use the default action. • Set `discard` to accept the message and delete it without informing the sending system. • Set `forward` to have messages forwarded to the email address set with the `emailaddr` keyword of the`set out_profile profile modify actions` command. • Set `reject` to reject the message and return an error to the sending system. • Set `review` to divert spam to the system quarantine. • Set `subject` to tag the message subject.	`default`

History

FortiMail v3.0 New.

Related topics

- set out_profile profile modify actions

out_profile profile modify scanoptions

Use these commands to configure scanning options for an outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify scanoptions attachment_type pdf
  {enable | disable}
set out_profile profile <name_str> modify scanoptions bypass_on_auth
  {enable | disable}
set out_profile profile <name_str> modify scanoptions maxsize <size_int>
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`attachment_type pdf {enable | disable}`	Enable to allow the FortiMail unit scan the first page of PDF attachments. The PDF option allows the heuristic, banned word, and image spam scanning techniques to examine the contents of PDF files. If none of these three scanners are enabled, the PDF option will have no effect.	`disable`
`bypass_on_auth {enable | disable}`	Enable or disable the bypassing of spam scanning when an SMTP sender is authenticated.	`disable`
`maxsize <size_int>`	Enter the maximum message size, in bytes, that the FortiMail unit will scan for spam. Messages with sizes exceeding the set limit will not be scanned for spam. Enter 0 to scan all messages regardless of size.	`0`

History

FortiMail v3.0	New.
FortiMail v3.0 MR1	`attachment_type pdf` added.

Related topics

- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify surbl

Use this command to enable or disable the checking of mail against defined SURBL servers for an outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify surbl {enable | disable}
```

`<name_str>` is the name of the profile. By default, SURBL scanning is disabled.

History

FortiMail v3.0	New.

Related topics

- set out_profile profile modify surblserver
- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify surblserver

Use these commands to configure the SURBL server list for an outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify surblserver <host_str> add
set out_profile profile <name_str> modify surblserver <host_str> delete
set out_profile profile <name_str> modify surblserver <host_str> move-to
  <new_int>
set out_profile profile <name_str> modify surblserver <host_str>
  rename-to <new_str>
```

Keywords and variables	Description
`<name_str>`	Enter the name of the antispam profile to modify.
`<host_str>`	Enter the host name SURBL server entry you want to modify.
`add`	Add the new SURBL server.
`delete`	Delete the SURBL server.
`move-to <new_int>`	Change the position of the SURBL server in the server list. Each entry is numbered, the first is 1, the second 2, and so on. `<new_int>` is the entry's new position.
`rename-to <new_str>`	Change the SURBL server host name.

History

FortiMail v3.0	New.

Related topics

- set out_profile profile modify surbl
- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify tags

Use these commands to configure header and subject tagging for an outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify tags header {enable | disable}
set out_profile profile <name_str> modify tags htag <tag_str>
set out_profile profile <name_str> modify tags stag <tag_str>
set out_profile profile <name_str> modify tags subject {enable | disable}
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`header {enable | disable}`	Enable or disable header tagging for the specified profile. A header tag must be set before header tagging can be enabled.	`disable`
`htag <tag_str>`	Enter the text added to the email header.	no default
`stag <tag_str>`	Enter the text added to the email subject.	no default
`subject {enable | disable}`	Enable or disable subject tagging for the specified profile.	`disable`

History

FortiMail v3.0	New.

Related topics

- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify virus

Use this command to enable or disable treating messages with a virus as spam.

Syntax

```
set out_profile profile <name_str> modify virus {enable | disable}
```

`<name_str>` is the name of the profile. By default, this setting is disabled.

History

FortiMail v3.0	New.

Related topics

- set out_profile profile modify actions
- set out_profile profile modify individualaction scanner

out_profile profile modify whitelistword

Use this command to enable or disable whitelist word checking in the specified outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> modify whitelistword
  {enable | disable}
```

By default, this setting is disabled.

History

FortiMail v3.0 MR3 New.

Related topics

- set out_profile profile modify whitelistwordlist

out_profile profile modify whitelistwordlist

Use this command to add, delete, or modify whitelist words for the specified antispam profile.

Syntax

```
set out_profile profile <name_str> modify whitelistwordlist <word_str>
  add subject {enable | disable} body {enable | disable}
set out_profile profile <name_str> modify whitelistwordlist <word_str>
  change body {enable | disable}
set out_profile profile <name_str> modify whitelistwordlist <word_str>
  change subject {enable | disable}
set out_profile profile <name_str> modify whitelistwordlist <word_str>
  change word <new_str>
set out_profile profile <name_str> modify whitelistwordlist <word_str>
  delete
set out_profile profile <name_str> modify whitelistwordlist <word_str>
  move-to <dest_int>
```

Keywords and variables	Description	Default
`<name_str>`	Enter the name of the antispam profile to modify.	
`<word_str>`	Enter the whitelist word.	
`add subject {enable	disable} body {enable	disable}`	Add the specified word as a whitelist word. Enable or disable checking of the message subject and body for the whitelist word.	
`change body {enable	disable}`	Select whether the email body text is examined for whitelist words.	`disable`
`change subject {enable	disable}`	Select whether the email subject text is examined for whitelist words.	`disable`
`change word <new_str>`	Change the specified whitelist word. The `<name_str>` variable specifies the existing word and `<new_str>` is the new word.	
`delete`	Delete the specified whitelist word	
`move-to <dest_int>`	Move the specified word to the position in the whitelist word list specified by the `<dest_int>` variable.	

History

FortiMail v3.0 MR3 New.

Related topics

- set out_profile profile modify whitelistword

out_profile profile rename-to

Use this command to rename an outgoing antispam profile.

Syntax

```
set out_profile profile <name_str> rename-to <new_str>
```

`<name_str>` is the name of the outgoing antispam profile.

Keywords and variables	Description
`<name_str>`	Enter the name of the outgoing antispam profile to rename.
`rename-to <new_str>`	Enter the new name of the outgoing antispam profile.

History

FortiMail v3.0	New.

Related topics

- set out_profile profile delete

policy delete

Use this command to remove the specified policy. This command is available in gateway and transparent modes only.

Syntax

```
set policy <fqdn_str> delete
```

History

FortiMail v3.0	New.

Related topics

- set policy modify rename-to

policy modify add_association

Use this command to configure domain associations.A domain association is a domain name that uses all the settings configured for the domain it is associated with. Domain associations are defined within domains or subdomains you have created.

Domain associations are only supported in gateway and transparent modes.

For example, if you have a mail server handling the email for three domains, one way to configure the FortiMail unit would be to create three separate domains and configure them all with the same settings. Another way is to configure one domain and add the other two to the first as domain associations. Subsequent configuration changes need to be made only once to apply to the domain and all domain associations.

Syntax

```
set policy <fqdn_str> modify add_association <fqdn>[, <fqdn>, <fqdn>,
  <fqdn>, ...]
```

Keywords and Variables	Description
`policy <fqdn_str>`	Enter the domain to which the associations will be added.
`add_association <fqdn>`	Enter the domain association. Enter multiple domains separated by commas.

History

FortiMail v3.0 MR4 New.

policy modify bverify_addr

Use this command to enable or disable background address verification for the specified domain. This command is available in gateway and transparent modes only.

Syntax

```
set policy <fqdn_str> modify bverify_addr <disable | ldap | smtp>
```

`<disable | ldap | smtp>` - choose LDAP or SMTP to enable background address verification using that method, or disable to deactivate this feature.

History

FortiMail v3.0	New.

Related topics

- set policy modify verify_addr

policy modify fallback

Use this command to set the fallback host for the specified domain. An optional fallback host port number may be specified. This command is available in gateway and transparent modes only.

Syntax

```
set policy <fqdn_str> modify fallbackhost <host_ipv4>
  [fallbackport <port_int>]
```

Keywords and Variables	Description
`fallbackhost <host_ipv4>`	Enter the IP address of the fallback host for this domain.
`fallbackport <port_int>`	Optionally, enter the fallback host port number.

History

FortiMail v3.0	New.

policy modify ip

Use this command to set the SMTP server IP of the email server for the specified domain. This command is available in gateway and transparent modes only.

Syntax

```
  set policy <fqdn_str> modify ip <server_ipv4>
```

```
<server_ipv4> - the IP address of the email server for this domain.
```

History

FortiMail v3.0	New.

policy modify is_subdomain

Use this command to set whether the specified domain is a subdomain. This command is available in gateway and transparent modes only.

Enable `is_subdomain` to declare this domain a subdomain.

Syntax

```
set policy <fqdn_str> modify is_subdomain {enable | disable}
```

History

FortiMail v3.0	New.

policy modify ldap

Use this command to set up LDAP based authentication for:

- antispam and antivirus configuration checking for the specified domain
- checking of routing configuration for the specified domain

This command is available in gateway and transparent modes only.

Syntax

To set the LDAP profile to use for LDAP antispam and antivirus queries:

```
set policy <fqdn_str> modify ldapasav profile <profile_str>
```

To enable or disable LDAP antispam and antivirus configuration checking:

```
set policy <fqdn_str> modify ldapasav state {enable | disable}
```

To set the LDAP profile to use for LDAP routing configuration:

```
set policy <fqdn_str> modify ldaprouting profile <profile_str>
```

To enable or disable LDAP routing configuration:

```
set policy <fqdn_str> modify ldaprouting state {enable | disable}
```

Keywords and Variables	Description
`<fqdn_str>`	Enter the fully qualified domain name.
`<profile_str>`	Enter the profile name.

History

FortiMail v3.0 New.

policy modify mxflag

Use this command to enable or disable the use of MX record for this domain. This command is available in gateway and transparent modes only.

Syntax

```
set policy <fqdn_str> modify mxflag {0 | 1}
```

Setting `mxflag` to 0 enables the MX record for this domain.

`<fqdn_str>` is the fully qualified domain name.

History

FortiMail v3.0	New.

policy modify tp

Use this command to configure transparent mode settings including transparent mode masquerading setting. This command is available only in transparent mode.

Syntax

```
set policy <fqdn_str> modify tp <zone_intr> {yes | no} {yes | no}
```

Keywords and Variables	Description	Default
`<fqdn_str>`	Enter the fully qualified domain name.	No default.
`<zone_intr>`	Specify which zone this domain is in with <zone_intr>. This determines the interface used to send and receive mail to this domain.	`0`
`{yes | no}`	Specify “yes” to hide this FortiMail unit or “no” to not hide it. This is the Transparent mode masquerading setting.	`no`
`{yes | no}`	Specify “yes” to use the SMTP server for the this domain, or “no” to relay the mail for this domain. The default is “no’.	`no`

History

FortiMail v3.0 New.

policy modify user

Use this command to configure recipient-based policies. This command is available in gateway and transparent modes only.

Syntax

```
set policy <fqdn_str> modify user <user_str> delete
set policy <fqdn_str> modify user <user_str> modify as <name_str>
set policy <fqdn_str> modify user <user_str> modify av <name_str>
set policy <fqdn_str> modify user <user_str> modify content <name_str>
set policy <fqdn_str> modify user <user_str> rename-to <newuser_str>
```

Keywords and Variables	Description	Default
`<fqdn_str>`	Enter the fully qualified domain name.	
`<user_str>`	Enter the recipient-based policy user ID.	
`delete`	Deletes the specified recipient-based policy.	
`modify as <name_str>`	Select the antispam profile to apply to the selected recipient-based policy.	`antispam_def`
`modify av <name_str>`	Select the antivirus profile to apply to the selected recipient-based policy.	`antivirus_def`
`modify content <name_str>`	Select the content profile to apply to the selected recipient-based policy.	`content_def`
`rename-to <newuser_str>`	Rename a recipient-based policy user ID. • `<newuser_str>` is the new user ID.	

History

FortiMail v3.0	New.

Related topics

- set policy delete
- set policy modify rename-to

policy modify verify_addr

Use this command to enable or disable recipient address verification. This command is available in gateway and transparent modes only.

Syntax

```
set policy <fqdn_str> modify verify_addr {ldap | smtp | disable} profile
  <name_str>
```

Keywords and Variables	Description	Default
`<fqdn_str>`	Enter the fully qualified domain name.	No default.
`verify_addr {ldap | smtp | disable}`	Choose LDAP or SMTP to enable background address verification using that method, or disable to deactivate this feature.	`disable`
`profile <name_str>`	Enter the name of the profile to use for this feature.	No default.

History

FortiMail v3.0 New.

Related topics

- set policy modify bverify_addr

policy modify rename-to

Use this command to rename the specified domain to the new domain name. This command is available in gateway and transparent modes only.

Syntax

```
set policy <fqdn_str> rename-to <newfqdn_str>
```

History

FortiMail v3.0	New.

Related topics

- set policy delete

spam deepheader

Use this command to configure the header analysis settings of the deep header scan feature.

Syntax

```
set spam deepheader confidence <confidence_int>
```

Keywords and Variables	Description	Default
`confidence <confidence_int>`	Enter the confidence value above which a message will be considered spam. The header analysis scan will examine 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 header analysis adds an `X-FEAS-DEEPHEADER` line to the message header that includes the message's calculated confidence value.	`95.0000`

History

FortiMail v3.0 MR1	New.
FortiMail v3.0 MR3	Removed `iptrusted` and `servertrusted` keywords.

Related topics

- set as profile modify deepheader
- set out_profile profile modify deepheader
- get spam deepheader

spam retrieval policy

Use this command to enable or disable authentication for a user on the specified domain to retrieve spam from the FortiMail unit using POP3 or HTTP.

Syntax

```
set spam retrieval policy <fqdn_str> user <user_str>
  auth {imap | ldap | pop3 | radius | smtp} <profile_str>
  senddomain {enable | disable} [allowaccess {pop3 http smtpauth
  diffident}]
```

Keywords and Variables	Description	Default
`<fqdn_str>`	Enter the user's domain.	
`<user_str>`	Enter the user's ID with the domain, e.g. user1@example.com. Entering the user ID without the domain will result in the command returning an error.	
`auth {imap | ldap | pop3 | radius | smtp}`	Select the type of server used for authentication.	
`<profile_str>`	Enter the authentication profile name.	
`senddomain {enable | disable}`	Enable to send the domain name with the user's ID to the authentication server.	`disable`
`[allowaccess {pop3 http smtpauth diffident}]`	Select the type of access allowed. • `{pop3}` allows POP3 retrieval of spam messages. • `{http}` allows webmail viewing and retrieval of spam messages. • `{smtpauth}` enables SMTP authentication. • `{diffident}` allows different sender identity.	

History

FortiMail v3.0 New.

Related topics

- set as control autorelease

system admin

Use this command to create or edit a system admin on your FortiGate system. Using this command you can set:

- the administrator’s password
- the administrator’s permission level
- the administrator’s trusted hosts which determine which network addresses the administrator can use to access the FortiMail unit

Syntax

```
set system admin username <name_str> domain <domain_str>
  password <password_str> permission {readonly | readwrite}
  sshkey {<key_str> | ‘remove’} trusthost <trusthost_ipmask>
  webmode {basic | advanced}
```

Keywords and Variables	Description
`username <name_str>`	Enter the name of the administrator account being created or edited.
`domain <domain_str>`	Enter the domain the administrator belongs to.
`password <password_str>`	Enter the password for the administrator account.
`permission {readonly	readwrite}`	Select administrator permission. `readonly` allows the administrator to only inspect settings, while `readwrite` also allows changing settings.
`sshkey (<key_str> | ‘remove’)`	Enter the SSH key string for the admin user. Enter ‘remove’ to remove the current SSH key.
`trusthost <trust_ipmask>`	Enter the host address and netmask from which the administrator can log in to the web-based manager. If you want the administrator to be able to access the FortiMail unit from any address, set `<trust_ipmask>` to 0.0.0.0 0.0.0.0.
`webmode (basic | advanced)`	Select either basic or advanced interface mode as the default webmode interface when logging in to this admin account.

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Added `sshkey` and `webmode` keywords.

Related topics

- set system option
- set user

system appearance

Use this command to customize the appearance of your FortiMail unit. Using this command you can change:

- the look of the bottom logo on the GUI
- the product name on main login screen
- the language of the webmail interface
- the title of the login for webmail
- the text of the prompt to enter your email address for webmail

Syntax

```
set system appearance [bottom-logo-url <bottom-logo-url>]
  [product <product_name_str>] [webmail_lang <language>]
  [webmail_login <webmail_str>] [webmail_login help <hint_str>]
```

Keywords and Variables	Description
`bottom-logo-url <image-url>`	Enter the URL of the image to be displayed at the bottom left of the FortiMail GUI status bar.
`product <product_name_str>`	Enter the name that will precede ‘Administrator Login’ on the FortiMail login page.
`webmail_lang <language>`	Select the language to use for the Webmail interface displayed to the user. Select the language from the list provided: • English • Chinese Simplified • Chinese Traditional • Korean • Japanese • French • German • Italian • Hebrew • Spanish • Polish • Portuguese • Turkish
`webmail_login <webmail_str>`	Enter the name or phrase that will precede the ‘Username’ prompt when logging in to webmail.
`webmail_login_hint <hint_str>`	Enter the text used to prompt the user to input their email address. By default the prompt is “Input your email address”.

History

FortiMail v3.0 New.

FortiMail v3.0 MR3 Added `webmail_lang` and `webmail_login_hint` keywords.

Related topics

- set console

system autoupdate pushaddressoverride

Use this command to change the IP address and port the FDN server sends updates on. This IP address will be different from the management IP address, the default address FDN connects to.

If the FDN can connect to the FortiMail unit only through a NAT device, you must configure port forwarding on the NAT device and add the port forwarding information to the push update configuration. Using port forwarding, the FDN connects to the FortiMail unit using either port 9443 or an override push port that you specify.

Push updates are provided to the FortiMail unit from the FDN using HTTPS on UDP port 9443. To receive push updates, the FDN must be able to route packets to the FortiMail unit using UDP port 9443. Any incoming traffic will arrive at the NAT device on <port_int> but must be resent to the FortiMail unit on port 9443.

Note: You cannot receive push updates through a NAT device if the external IP address of the NAT device is dynamic (for example, set using DHCP).

Syntax

To change the FDN push update address and port

```
set system autoupdate pushaddressoverride enable <addr_ip4> <port_int>
```

To disable override of default FDN address

```
set system autoupdate pushaddressoverride disable
```

<addr_ip4> is the IP address of the NAT device in front of the FortiMail unit.

<port_int> is the port on the NAT device that will receive updates.

History

FortiMail v3.0	New.

Related topics

- set system autoupdate pushupdate
- set system autoupdate schedule
- set system autoupdate tunneling

system autoupdate pushupdate

Use this command to enable or disable push updates from the Fortinet Distribution Network (FDN).

Syntax

```
set system autoupdate pushupdate {enable | disable}
```

History

FortiMail v3.0	New.

Related topics

- set system autoupdate pushaddressoverride
- set system autoupdate schedule
- set system autoupdate tunneling

system autoupdate schedule

Use this command to schedule updates.

Syntax

To schedule updates every set amount of hours and minutes,

```
set system autoupdate schedule {enable | disable} every <hh:mm>
```

To schedule updates daily,

```
set system autoupdate schedule {enable | disable} daily <hh:mm>
```

To schedule updates weekly,

```
set system autoupdate schedule {enable | disable} weekly <day_int>
  <hh:mm>
```

For an interval of ‘every’, ‘<hh:mm>’ is the period between updates. For example if <hh:mm> was 3:45, every 3 hours and 45 minutes the FortiMail unit would check for updates.

For an interval of ‘daily’, ‘<hh:mm>’ is the time of day to get updates. For example if <hh:mm> was 3:45, every day at 3:45am the FortiMail unit would check for updates. 15:45 would be 3:34pm.

For an interval of ‘weekly’, the seven days of the week is indicated by <day_int>, with 0 being Sunday, and 6 being Saturday. ‘<hh:mm>’ has the same meaning as for the daily interval. For example ‘ weekly 2 15:45’ would indicate to get updates once per week on Tuesdays at 15:45pm.

History

FortiMail v3.0	New.

Related topics

- set system autoupdate pushaddressoverride
- set system autoupdate pushupdate
- set system autoupdate tunneling

system autoupdate tunneling

Use this command to configure web proxy tunneling.

Syntax

```
set system autoupdate tunneling {enable | disable} address <addr_ip4>
  port <port_num> username <username_str> password <pwd_str>
```

Keywords and Variables	Description
`address <addr_ip4>`	Enter the proxy IP address.
`port <port_num>`	Enter proxy port to use.
`username <username_str>`	Enter the web proxy user name.
`password <pwd_str>`	Enter the web proxy password.

History

FortiMail v3.0	New.

Related topics

- set system autoupdate pushaddressoverride
- set system autoupdate pushupdate
- set system autoupdate schedule

system ddns

Use this command to configure Dynamic DNS for this interface. Set the domain and username using separate commands.

Syntax

```
set system ddns server <server_name> domain <domain_str> ipmode {auto |
  bind interface <intf_str> | static ip <ipv4_int>} status {enable |
  disable}
set system ddns server <server_name> username <username_str> password
  <pwd_str> timeout <hours_int>
```

Keywords and Variables	Description
`server <server_name>`	Select the DDNS server from the list provided: • 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
`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 - auto detect the external IP address • bind - bind the IP address with a specific interface • static - a specific static IP address
`interface <intf_str>`	Enter the interface to bind the IP address to. Command only available when `ipmode bind` is selected.
`ip <ipv4_str>`	Enter the IP address to be the static address. Command only available when `ipmode static` is selected.
`status {enable | disable}`	Activate or disactivate this DDNS server.
`username <username_str>`	Enter the username to access this DDNS server.
`password <pwd_str>`	Enter the password to access this DDNS server.
`timeout <hours_int>`	Enter the interval in hours after which your FortiMail unit will contact the DDNS server to reaffirm your IP address.

History

FortiMail v3.0	New.

Related topics

- set system interface mode dhcp
- set system interface mode static

system disclaimer allowdomain

Use this command to enable per-domain disclaimer settings.

Syntax

```
set system disclaimer allowdomain {enable | disable}
```

History

FortiMail v3.0	New.

Related topics

- set system disclaimer incoming
- set system disclaimer outgoing

system disclaimer incoming

Use this command to configure incoming disclaimer messages. Disclaimer messages can be applied to either the body or header of an email.

Each can be enabled or disabled and has a content string.

Syntax

```
set system disclaimer incoming body status {enable | disable} content
  <content_str>
set system disclaimer incoming header status {enable | disable} content
  <content_str>
```

History

FortiMail v3.0	New.

Related topics

- set system disclaimer allowdomain
- set system disclaimer outgoing

system disclaimer outgoing

Use this command to configure outgoing disclaimer messages. Disclaimer messages can be applied to either the body or header of an email.

Each can be enabled or disabled and has a content string.

Syntax

```
set system disclaimer outgoing body status {enable | disable} content
  <content_str>
set system disclaimer outgoing header status {enable | disable} content
  <content_str>
```

History

FortiMail v3.0	New.

Related topics

- set system disclaimer allowdomain
- set system disclaimer incoming

system dns

Use this command to the DNS addresses and behavior.

Syntax

```
set system dns cache {enable | disable} primary {<addr_ip4> | none}
  private_ip_query {enable | disable} secondary {<addr_ip4> | none}
```

Keywords and Variables	Description
`cache {enable | disable}`	Enable DNS caching to speed up resolving domain names. Disable the DNS cache to free memory if you are low on memory.
`primary { <addr_ip4> | none}`	Enter the IP address of the primary DNS server. Enter ‘none’ to delete the primary DNS server entry.
`private_ip_query {enable | disable}`	Enable private IP queries to perform a reverse DNS lookup on private IP addresses such as 192.168.0.0/16. This is the default Disable private IP queries if reverse DNS lookups take too long to return ‘host not found’ for private IP addresses with no PTR record on the DNS server.
`secondary { <addr_ip4> | none}`	Enter the IP address of the secondary DNS server. Enter ‘none’ to delete the secondary DNS server entry.

History

FortiMail v3.0	New.
FortiMail v3.0 MR3	Added `cache` and `private_ip_query` keywords.

Related topics

- set system interface config
- set system interface mode dhcp
- set system route number

system fortimanager

Use this command to configure FortiManager support.

Syntax

```
set system fortimanager autobackup {enable | disable}
set system fortimanager central-management {enable | disable}
set system fortimanager initiate {enable | disable}
set system fortimanager ip <ipv4>
```

Keywords and Variables	Description
`autobackup {enable | disable}`	When enabled, the FortiMail unit will send a configuration backup to the FortiManager unit every time an administrator logs out of the FortiMail web-based manager. The FortiManager units saves these configuration backup files.
`central-management {enable | disable}`	Enable to allow a FortiManager unit to manage your FortiMail unit.
`initiate {enable | disable}`	When enabled, the FortiMail unit accepts configuration updates from the FortiManager unit.
`ip <ipv4>`	Enter the IP address of the FortiManager unit.

History

FortiMail v3.0 MR4 New.

Related topics

- set system interface config
- set system interface mode dhcp
- set system route number

system ha config

Use this command to change the TCP port and time interval for synchronizing the FortiMail configuration.

Note: Use the `set system ha config` command to configure HA daemon settings. Other HA daemon configuration commands include “set system ha data” on page 318, “set system ha datadir” on page 319, “set system ha monitor” on page 322, and “set ” on page 324.

In most cases you do not have to change the default settings. However if you are making a lot of configuration changes, you may want to reduce the time between synchronizations so that changes are not lost if a failover occurs. The default `<timeout_integer>` is 60 minutes. During normal operation, synchronizing the configuration once every 60 minutes is usually sufficient.

You can also synchronize the configuration manually. See “set system ha {restart | restore | resync}” on page 327.

For more information about how FortiMail HA synchronizes the configuration and about what is synchronized and what is not synchronized, see the *FortiMail Administration Guide*.

Syntax

```
set system ha config <port_integer> <timeout_integer>
```

Keywords/Variables	Description	Default
`<port_integer>`	The TCP port used for synchronizing the configuration of the primary unit to the backup unit.	`20001`
`<timeout_integer>`	How often HA synchronizes the configuration. The minimum `<timeout_integer>` is every 15 minutes. The maximum configuration synchronization time is 999 minutes. If `<timeout_integer>` is set to 0 the configuration is not synchronized.	`60`

Example

Enter the following command to set the FortiMail configuration synchronization time interval to 30 minutes. The command maintains the default value of the synchronization port as 20001.

```
set system ha config 20001 30
```

History

FortiMail v3.0	New.

Related topics

- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha data
- set system ha datadir
- set system ha lservice
- set system ha mode
- set system ha monitor
- set system ha on-failure
- set system ha passwd
- set system ha remote-as-heartbeat
- set system ha {restart | restore | resync}
- set system ha rservice
- set system ha takeover

system ha {cpeer | interface | peer | secondary-interface | secondary-peer}

Use these commands to configure primary heartbeat interface settings for FortiMail active-passive and config only HA groups. You can also use these commands to optionally configure the secondary heartbeat interface settings for FortiMail active-passive HA.

For an active-passive or a config only HA group, use the `set system ha interface` command to select the network interface to be used for the primary heartbeat and to configure the primary heartbeat local IP address and netmask.

For a config only HA group use the `set system ha cpeer` command to add the IP address of a backup unit (also called a peer) to the known peers list or to change the IP address of a backup unit already added to the known peers list. The primary unit requires these IP addresses to be able to communicate with the backup units.

For an active-passive HA group use the `set system ha peer` command to configure the primary heartbeat peer IP address.

For an active-passive HA group use the `set system ha secondary-interface` command to configure the network interface to be used for the secondary heartbeat and to configure the secondary heartbeat local IP address and netmask. You can specify an interface name, disable the secondary heartbeat, or set the secondary heartbeat to `any` if you don’t want to use a specific interface as the backup heartbeat interface. `any` means that any interface with its HA interface configuration set to ignore this interface using the `set system ha takeover <interface_str> ignore` command can be used as the secondary heartbeat interface.

For an active-passive HA group use the `set system ha secondary peer` command to configure the secondary heartbeat peer IP address.

Syntax

```
set system ha cpeer <cpeer_integer> <cpeer_ipv4>
set system ha interface <primary-interface_str> <primary-local_ipv4>
  <netmask_ipv4>
set system ha peer <primary-peer_ipv4>
set system ha secondary-interface {<secondary-interface_str> | any |
  disabled} <secondary-local_ipv4> <netmask_ipv4>
set system ha secondary-peer <secondary-peer_ipv4>
```

Keywords/Variables	Description	Default
`any`	Set the secondary heartbeat interface to use any interface that has been set to `ignore` using the `set system ha takeover` command.	
`disabled`	Disable the secondary heartbeat interface.	
`<cpeer_integer>`	The number of the backup unit in the known peers list. You can add up to 24 backup units or peers.	
`<cpeer_ipv4>`	The IP address of the config only peer unit. In a config only HA group you would normally set `10.0.0.2` as the peer IP address for the first backup unit, `10.0.0.3` as the peer IP address for the second backup unit, `10.0.0.4` as the peer IP address for the third backup unit, and so on.	

Keywords/Variables	Description	Default

`<primary-local_ipv4> <netmask_ipv4>`	The primary heartbeat local IP address and netmask for this FortiMail unit. When the FortiMail unit is operating in HA mode, you can enter `get system interface <interface_str>` to display this IP address and netmask, where `<interface_str>` is the name of the primary heartbeat interface.
	`primary-local_ipv4` of the primary unit must match `primary-peer_ipv4` of the backup unit. Normally you would set `primary-local_ipv4` on the primary unit to `10.0.0.1`.
	In an active-passive HA group `primary-local_ipv4` of the backup unit must match `primary-peer_ipv4` of the primary unit. Normally you would set `primary-local_ipv4` on the backup unit to `10.0.0.2`.
	In a config only HA group you would normally set `primary-local_ipv4` on the first backup unit to `10.0.0.2`, `primary-local_ipv4` on the second backup unit to `10.0.0.3`, `primary-local_ipv4` on the third backup unit to `10.0.0.4`, and so on.
		`10.0.0.1`
		`255.255.255.0`

`<primary-interface_str>`	The name of the network interface to be used for the primary heartbeat. The default primary heartbeat interface is the network interface with the highest number. In most cases you would not have to select a different network interface.	

`<primary-peer_ipv4>`	The primary heartbeat IP address for the other FortiMail unit in the HA group. This is the IP address that the FortiMail unit primary heartbeat expects to be able to connect to find the other FortiMail unit in the HA group.
	`primary-peer_ipv4` of the primary unit must match the `primary-local_ipv4` of the backup unit. Normally you would set `primary-peer_ipv4` on the primary unit to `10.0.0.2`.
	`primary-peer_ipv4` of the backup unit must match the `primary-local_ipv4` of the primary unit. For an active-passive or a config only HA group you would set `primary-peer_ipv4` of the backup unit or units to `10.0.0.1`.
		`10.0.0.2`
		`255.255.255.0`

`<secondary-local_ipv4> <netmask_ipv4>`	In an active-passive HA group, the secondary heartbeat local IP address and netmask for this FortiMail unit. When the FortiMail unit is operating in HA mode, you can enter `get system interface <interface_str>` to display this IP address and netmask, where `<interface_str>` is the name of the secondary heartbeat interface. `secondary-local_ipv4` of the primary unit must match `secondary-peer_ipv4` of the backup unit. You could set `secondary-local_ipv4` on the primary unit to `10.1.1.1`. `secondary-local_ipv4` of the backup unit must match `secondary-peer_ipv4` of the primary unit. You could set `primary-local_ipv4` on the backup unit to `10.1.1.2`.	`0.0.0.0` `0.0.0.0`

Keywords/Variables	Description	Default
`<secondary-interface_str>`	The name of the network interface to be used for the secondary heartbeat.	
`<secondary-peer_ipv4>`	The secondary heartbeat IP address for the other FortiMail unit in the HA group. This is the IP address that the FortiMail unit secondary heartbeat expects to be able to connect to find the other FortiMail unit in the HA group. `secondary-peer_ipv4` of the primary unit must match the `secondary-local_ipv4` of the backup unit. You could set the `secondary-peer_ipv4` on the primary unit to `10.1.1.2`. `secondary-peer_ipv4` of the backup unit must match the `secondary-local_ipv4` of the primary unit. You could set the `secondary-peer_ipv4` of backup unit to `10.1.1.1`.	`0.0.0.0` `0.0.0.0`

Example: configuring primary heartbeat local and peer IP address for a config only HA group

This example describes how to configure primary local and peer IP addresses for a config only HA group consisting of one primary unit and three backup units.

- Enter the following commands from a config only HA primary unit to set `port5` as the primary heartbeat interface, set the primary local HA heartbeat IP address and netmask to 10.0.0.1 255.255.255.0, and add three backup units to the peer list. The primary heartbeat local addresses of the backup units to be added to the peer list are 10.0.0.2, 10.0.0.3, and 10.0.0.4.

  ```
  set system ha interface port5 10.0.0.1 255.255.255.0
  set system ha cpeer 1 10.0.0.2
  set system ha cpeer 2 10.0.0.3
  set system ha cpeer 3 10.0.0.4
  ```

- Enter the following command from the first config only HA backup unit to set `port5` as the primary heartbeat interface and set the primary heartbeat local IP address and netmask to 10.0.0.2 255.255.255.0.

  ```
  set system ha interface port5 10.0.0.2 255.255.255.0
  ```

- Enter the following command from the second config only HA backup unit to set `port5` as the primary heartbeat interface and set the primary heartbeat local IP address and netmask to 10.0.0.3 255.255.255.0.

  ```
  set system ha interface port5 10.0.0.3 255.255.255.0
  ```

- Enter the following command from the third config only HA backup unit to set `port5` as the primary heartbeat interface and set the primary heartbeat local IP address and netmask to 10.0.0.4 255.255.255.0.

  ```
  set system ha interface port5 10.0.0.4 255.255.255.0
  ```

Example: configuring primary heartbeat local and peer IP address for an active-passive HA group

This example describes how to configure primary heartbeat local and peer IP addresses for an active-passive HA group consisting of one primary unit and one backup unit.

Enter the following commands from an active-passive HA primary unit to set `port5` as the primary heartbeat interface, set the primary heartbeat local IP address and netmask to 10.0.0.1 255.255.255.0, and set the primary heartbeat peer IP address to 10.0.0.2.

```
set system ha interface port5 10.0.0.1 255.255.255.0
set system ha peer 10.0.0.2
```

Enter the following commands from an active-passive HA backup unit to set `port5` as the primary heartbeat interface, set the primary heartbeat local heartbeat interface IP address and netmask to 10.0.0.2 255.255.255.0, and set the primary heartbeat peer IP address to 10.0.0.1.

```
set system ha interface port5 10.0.0.2 255.255.255.0
set system ha peer 10.0.0.1
```

Example: add a secondary heartbeat local and peer IP address for an active-passive HA group

This example adds a secondary heartbeat local and peer IP addresses to the FortiMail units in the previous example.

Enter the following commands from an active-passive HA primary unit to set `port4` as the secondary heartbeat interface, set the secondary heartbeat local IP address and netmask to 10.1.1.1 255.255.255.0, and set the secondary heartbeat peer IP address to 10.1.1.2.

```
set system ha secondary-interface port4 10.1.1.1 255.255.255.0
set system ha secondary-peer 10.1.1.2
```

Enter the following commands from an active-passive HA backup unit to set `port4` as the secondary heartbeat interface, set the secondary heartbeat local heartbeat interface IP address and netmask to 10.1.1.2 255.255.255.0, and set the secondary heartbeat peer IP address to 10.1.1.1.

```
set system ha secondary-interface port4 10.1.1.2 255.255.255.0
set system ha secondary-peer 10.1.1.1
```

History

FortiMail v3.0	New.
FortiMail v3.0 MR2	Added `secondary-interface` and `secondary-peer` keywords that you use for configuring secondary heartbeat settings. In previous versions of FortiMail you used the `interface` and `peer` keywords for configuring HA heartbeat settings. In FortiMail v3.0 MR2 you use the `interface` and `peer` keywords for configuring primary heartbeat settings.

Related topics

- set system ha config
- set system ha data
- set system ha datadir
- set system ha lservice
- set system ha mode
- set system ha monitor
- set system ha on-failure
- set system ha passwd
- set system ha remote-as-heartbeat
- set system ha {restart | restore | resync}
- set system ha rservice
- set system ha takeover

system ha data

Use this command to set the TCP port and time interval for synchronizing FortiMail data.

Note: Use the `set system ha config` command to configure HA daemon settings. Other HA daemon configuration commands include "set system ha config" on page 313, "set system ha datadir" on page 319, "set system ha monitor" on page 322, and "set " on page 324.

In most cases you do not have to change the default settings. You might want to reduce the synchronization time if you find you are losing mail data during a failover. Also, synchronizing large amounts of mail data may cause processing delays. Reducing how often mail data is synchronized may alleviate this problem. The default `<timeout_integer>` is 30 minutes. During normal operation, synchronizing data once every 30 minutes is usually sufficient.

You can also synchronize the configuration manually. See "set system ha {restart | restore | resync}" on page 327.

You should disable mail data synchronization if the HA group stores mail data on a remote NAS server. See see the *FortiMail Administration Guide* for more information about HA and storing mail data on a remote NAS server.

Syntax

```
set system ha data <data_port_integer> <timeout_integer>
```

Keywords/Variables	Description	Default
`<data_port_integer>`	The TCP port used for synchronizing FortiMail data.	`20002`
`<timeout_integer>`	How often data synchronization occurs. The minimum `<timeout_integer>` 15 minutes. The maximum data synchronization time is 999 minutes. If `<timeout_integer>` is set to `0` data is not synchronized.	`30`

Example

Enter the following command to set the FortiMail data synchronization time interval to 100 minutes. The command maintains the default value of the synchronization port as 20002.

```
set system ha config 20002 100
```

History

FortiMail v3.0 New.

Related topics

- set system ha config
- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha datadir
- set system ha lservice
- set system ha mode
- set system ha monitor
- set system ha on-failure
- set system ha passwd
- set system ha remote-as-heartbeat
- set system ha {restart | restore | resync}
- set system ha rservice
- set system ha takeover

system ha datadir

Use this command to enable or disable synchronizing FortiMail mail data including the system mail directory, user home directories, and the MTA spool directories (FortiMail queues). Each time you enter this command you must enable or disable synchronizing all three types of mail data. Because the command does not include keywords, using the command involves entering the correct enable or disable sequence in the correct order as follows:

- First: enable or disable synchronizing the system mail directory.
- Second: enable or disable synchronizing the user home directories.
- Third: enable or disable synchronizing the MTA spool directories (FortiMail queues).

Synchronization of all three types of mail data is disabled by default.

Note: Use the `set system ha config` command to configure HA daemon settings. Other HA daemon configuration commands include "set system ha config" on page 313, "set system ha data" on page 318, "set system ha monitor" on page 322, and "set " on page 324.

Syntax

```
set system ha datadir {enable | disable} {enable | disable} {enable |
  disable}
```

Example

Enter the following command to:

- Enable synchronizing the system mail directory.
- Disable synchronizing the user home directories.
- Disable synchronizing the MTA spool directories (FortiMail queues).

```
set system ha datadir enable disable disable
```

History

FortiMail v3.0	New.

Related topics

- set system ha config
- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha data
- set system ha lservice
- set system ha mode
- set system ha monitor
- set system ha on-failure
- set system ha passwd
- set system ha remote-as-heartbeat
- set system ha {restart | restore | resync}
- set system ha rservice
- set system ha takeover

system ha lservice

Use this command to configure HA primary unit local services monitoring. Configure local service monitoring so that an active-passive HA primary unit monitors its own network interfaces and hard drives. You must configure how long in seconds to wait between checks of the interfaces or hard drives and how many times the check fails before a failover occurs.

Network interface monitoring monitors all active network interfaces. Network interfaces with their HA interface configuration set to ignore this interface are not monitored. For information about HA interface configuration, see "set system ha takeover" on page 330.

If the primary unit detects an interface failure (for example, if the network cable is disconnected from a monitored interface) or if the primary unit detects a hard drive failure, the primary unit HA effective operating mode changes to off.

If the primary unit effective operating mode changes to off, the primary unit no longer responds to HA heartbeat packets sent by the backup unit. The backup unit assumes that the primary unit has failed and becomes the new primary unit.

Syntax

```
set system ha lservice {ports | hd} <check_time_integer>
  <retries_integer>
```

Keywords/Variables	Description	Default
`{ports	hd}`	Enter `ports` to configure primary unit network interface monitoring. Enter hd to configure primary unit hard drive monitoring.	
`<check_time_integer>`	The check time interval in seconds to wait between checks of the interfaces or the hard drives. The check time interval range is 1 to 60 seconds. Set the check time interval to 0 to disable interface or hard drive monitoring.	`0`
`<retries_integer>`	The number of consecutive times interface monitoring or hard drive monitoring detects a failure before the primary unit changes its effective operating mode to off. The number of times the check fails range is 1 to a very high number. Set the number of times the check fails to 0 to disable interface monitoring or hard drive monitoring.	`0`

Example

Enter the following command to set primary unit interface monitoring to check the interfaces every 30 seconds and to change the primary unit effective operating mode to off if interface monitoring fails 10 consecutive checks.

```
set system ha lservice pprts 30 10
```

History

FortiMail v3.0	New.

Related topics

- set system ha config
- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha data
- set system ha datadir
- set system ha mode
- set system ha monitor
- set system ha on-failure
- set system ha remote-as-heartbeat
- set system ha {restart | restore | resync}
- set system ha rservice
- set system ha takeover

system ha mode

Use this command to set the HA configured operating mode of the FortiMail unit. The FortiMail unit switches to operating in the HA configured operating mode immediately after you enter this command.

Syntax

```
set system ha mode <mode>
```

Keywords/Variables	Description	Default
`mode <mode>`	Set the HA configured operating mode of the FortiMail unit. The configured operating mode can be: • `off` if the FortiMail unit is not operating in HA mode. • `master` if the FortiMail unit is the primary unit in an active-passive HA group. • `slave` if the FortiMail unit is the backup unit in an active-passive HA group. • `cmaster` if the FortiMail unit is the primary unit in a config only HA group. • `cslave` if the FortiMail unit is the backup unit in a config only HA group.	`off`

Example

Enter the following command to set the HA configured operating mode of a FortiMail unit to `cmaster`.

```
set system ha mode cmaster
```

History

FortiMail v3.0	New.

Related topics

- set system ha config
- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha data
- set system ha datadir
- set system ha lservice
- set system ha monitor
- set system ha on-failure
- set system ha passwd
- set system ha remote-as-heartbeat
- set system ha {restart | restore | resync}
- set system ha rservice
- set system ha takeover

system ha monitor

Use this command to configure how the FortiMail HA daemon sends HA heartbeat packets to detect if the primary unit has failed. If the backup unit detects that the primary unit has failed, the backup unit effective operating mode changes to master and the backup unit becomes the primary unit.

Note: Use the `set system ha config` command to configure HA daemon settings. Other HA daemon configuration commands include “set system ha config” on page 313, “set system ha data” on page 318, “set system ha datadir” on page 319, and “set ” on page 324.

In most cases you do not have to change heartbeat settings. The default settings mean that if the primary unit fails, the backup unit switches to being the primary unit after 3 x 5 or about 15 seconds; resulting in a failure detection time of 15 seconds.

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.

If the failure detection time is too short the backup unit may detect a failure when none has occurred. For example, if the primary unit is very busy processing email it may not respond to HA heartbeat packets in time. In this situation, the backup unit may assume that the primary unit has failed when the primary unit is actually just busy. Increase the failure detection time to prevent the backup unit from detecting a failure when none has occurred.

Syntax

```
set system ha monitor <heartbeat_port_integer> <heartbeat_time_integer>
  <retries)integer>
```

Keywords/Variables	Description	Default
`<heartbeat_port_integer>`	The TCP port used for HA heartbeat communications.	`20000`
`<heartbeat_time_integer>`	The time between which the FortiMail units in the HA group send HA heartbeat packets. The default test interval between HA heartbeat packets is 5 seconds. The test interval range is 2 to 60 seconds. Heartbeat packets are sent at regular intervals so that each FortiMail unit in an active-passive HA group can confirm that the other unit n the group is functioning. If the primary unit detects that the backup unit has failed the primary unit continues to operate normally. If the backup unit detects that the primary unit has failed, the HA effective operating mode of the backup unit changes to master and the back up unit becomes the primary unit.	5
`<retries_integer>`	The number of consecutive times the HA heartbeat detects a failure before the backup unit decides that the primary unit has failed. The number of times the check fails range is 1 to a very high number. Set the number of times the check fails to 0 to disable interface monitoring or hard drive monitoring.	

Example

Enter the following command to change the HA heartbeat configuration so that each FortiMail unit in the HA group send heartbeat packets every 20 seconds and the FortiMail units in the HA group detect a failure if the HA heartbeat check fails 5 times. This command keeps the HA heartbeat TCP port set to 20000.

```
set system ha monitor port 20000 20 5
```

History

FortiMail v3.0	New.

Related topics

- set system ha config
- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha data
- set system ha datadir
- set system ha lservice
- set system ha mode
- set system ha on-failure
- set system ha passwd
- set system ha remote-as-heartbeat
- set system ha {restart | restore | resync}
- set system ha rservice
- set system ha takeover

system ha on-failure

Use this command to control the behavior of a FortiMail unit in an active-passive HA group when remote service monitoring detects a failure. In most cases you should set On Failure to wait for recovery and then assume slave role. In this mode when service monitoring detects a failure the FortiMail unit effective operating mode changes to FAILED. In FAILED mode the FortiMail unit and can automatically recover, switch to the SLAVE effective operating mode and synchronize MTA spool directories with the other FortiMail unit which should be operating in the MASTER effective operating mode.

Syntax

```
set system ha on-failure {off | restore | slave}
```

Keywords/Variables	Description	Default
`off`	After a failure the FortiMail unit effective operating mode changes to OFF. The FortiMail unit will not process mail or join the HA group until you manually change the FortiMail unit effective operating mode to MASTER (primary) or SLAVE (backup).	
`restore`	Similar to `slave` the FortiMail unit effective operating mode changes to FAILED when remote service monitoring detects a failure. However, in this case on recovery the failed FortiMail unit effective operating mode switches back to its configured operating mode. This behavior may be useful in some scenarios but may cause problems in others.	
`slave`	The FortiMail unit effective operating mode changes to FAILED when remote service or local network interface service monitoring detects a failure. In FAILED mode the FortiMail unit uses remote service monitoring to attempt to connect to the other FortiMail unit in the HA group (which should be operating as the primary unit with effective operating mode of MASTER). If you fix the problem that caused the failure the failed FortiMail unit recovers by changing its effective operating mode to SLAVE. The failed FortiMail unit then synchronizes the content of its MTA spool directories to the FortiMail unit operating as the primary unit. The primary unit can then deliver this email.	

Example

Enter the following command to configure a FortiMail unit to switch to FAILED effective operating mode and when restored, to change the effective operating mode to SLAVE.

```
set system ha on-failure slave
```

History

FortiMail v3.0 MR2	New.

Related topics

- set system ha config
- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha data
- set system ha datadir
- set system ha lservice
- set system ha mode
- set system ha monitor
- set system ha passwd
- set system ha remote-as-heartbeat
- set system ha {restart | restore | resync}
- set system ha rservice
- set system ha takeover

system ha passwd

Use this command to Change HA group shared password.

Note: Use the `set system ha config` command to configure HA daemon settings. Other HA daemon configuration commands include "set system ha config" on page 313, "set system ha data" on page 318, "set system ha datadir" on page 319, and "set system ha monitor" on page 322.

In most cases you do not have to change any of the HA daemon settings. However you should change the shared password. The shared password is not synchronized and must be set separately on the primary and backup units.

Syntax

```
set system ha passwd <passwd_str>
```

Keywords/Variables	Description	Default
`<passwd_str>`	Enter a password for the HA group. The password must be the same on the primary and backup FortiMail units. The password must be a least 1 character.	`change_me`

Example

Enter the following command to set the shared password to `PassW4D`.

```
set system ha passwd Passw4D
```

History

FortiMail v3.0	New.

Related topics

- set system ha config
- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha data
- set system ha datadir
- set system ha lservice
- set system ha mode
- set system ha monitor
- set system ha on-failure
- set system ha remote-as-heartbeat
- set system ha {restart | restore | resync}
- set system ha rservice
- set system ha takeover

system ha remote-as-heartbeat

Use this command to enable or disable using remote monitoring as an HA heartbeat. Enable using remote monitoring as an HA heartbeat so that if both the primary and secondary heartbeat links fail, remote service monitoring takes over the role of the HA heartbeat. This means that if remote service monitoring is enabled and both heartbeat links fail or become disconnected, the FortiMail HA group can continue to operate.

Using remote services as heartbeat provides HA heartbeat only. HA synchronization is only supported using the primary or secondary heartbeat. To avoid synchronization problems, you should not use remote service monitoring as a heartbeat for extended periods. This feature is intended only as a temporary heartbeat solution that operates until you reestablish a normal primary or secondary heartbeat link.

Syntax

```
set system ha remote-as-heartbeat {enable | disable}
```

Example

Enter the following command to enable using remote monitoring as an HA heartbeat::

```
set system ha remote-as-heartbeat enable
```

History

FortiMail v3.0 MR2 New.

Related topics

- set system ha config
- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha data
- set system ha datadir
- set system ha lservice
- set system ha mode
- set system ha monitor
- set system ha on-failure
- set system ha passwd
- set system ha {restart | restore | resync}
- set system ha rservice
- set system ha takeover

system ha {restart | restore | resync}

Use these commands to execute commands on a FortiMail unit that control how the HA system operates. Using these commands you can:

- Restart the HA processes on the FortiMail unit.
- Restore the HA group to operate in the HA configured operating mode.
- Force the HA group to resynchronize configuration and mail data.

Syntax

```
set system ha {restart | restore | resync}
```

Keywords/Variables	Description	Default
`restart`	Restart all HA processes on the FortiMail unit from which you enter the command. You may need to restart the HA processes on a primary unit if HA local services monitoring or remote services monitoring has shut down the HA processes on the primary unit. Before restarting the HA processes you should find and correct the problem that caused the primary unit to be stopped.	
`restore`	If the HA configured operation mode and HA effective operating mode of a FortiMail unit in a HA group do not match, you can use this command to reset both units in the HA group to their HA configured operating modes. You can enter this command from the primary unit or the backup unit. Entering the command is only necessary if the normal operation of the HA group has been effected by a failure of some kind and you want to restore the HA group or one of the units in the HA group to normal operation. Before completing this procedure you should resolve any problems that could have caused a failure.	
`resync`	Use this command to force the primary unit to synchronize configuration changes and mail data to the backup unit or units. You can enter this command from the primary unit. This command can be used with an active-passive and a config only HA group. This command can be useful if you have made a number of configuration changes and you want to synchronize these configuration changes immediately instead of waiting for the configuration synchronization time interval to end.	

Example

Enter the following command to force the primary unit to resynchronize configuration changes to the backup unit or units.

```
set system ha resync
```

History

FortiMail v3.0	New.

Related topics

- set system ha config
- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha data
- set system ha datadir
- set system ha lservice
- set system ha mode
- set system ha monitor
- set system ha on-failure
- set system ha remote-as-heartbeat
- set system ha rservice
- set system ha takeover

system ha rservice

Use this command to configure HA backup unit remote services monitoring so that an active-passive HA backup unit monitors the primary unit to verify that the primary unit can accept SMTP service, POP service (POP3), and Web service (HTTP) connections.

For each protocol you must specify the check time interval in minutes to wait between checks and the response time to wait for a response. You must also specify how many times the check fails before the backup unit decides that the primary unit has failed and a failover occurs.

If the backup unit detects a remote services failure, the backup unit HA effective operating mode changes to master and the primary unit effective operating mode changes to off. The backup unit becomes the new primary unit.

Syntax

```
set system ha rservice {smtp | pop | imap | http} <interface_ipv4>
  <service_port_integer> <check_time_integer> <response_time_integer>
  <retries_integer>
```

Keywords/Variables	Description	Default
`{smtp | pop | imap | http}`	The service to configure remove service monitoring for. • `smtp` to configure SMTP remote service monitoring. • `pop` to configure POP3 remote service monitoring. • `imap` to configure IMAP remote service monitoring. • `http` to configure HTTP remote service monitoring.	
`<interface_ipv4>`	The IP address to connect to for testing each remote service. You can enter the same IP address or different IP addresses for each service. Normally you would enter the IP address of the FortiMail interface that processes email. If you add the IP address of the HA interface of the primary unit, checking takes place over the HA heartbeat link.	`0.0.0.0`
`<service_port_integer>`	The TCP port used for the service. In most cases `<service_port_integer>` would the standard TCP port for the service.	`0`
`<check_time_integer>`	The check time interval in seconds to wait between remote service checks. The check time interval range is 1 to 60 minutes. Set the check time interval to 0 to disable remote service monitoring.	`0`
`<response_time_integer>`	The response wait time in seconds to wait for a response to a remote service check. The response wait time range is 1 to a very high number of seconds. Set the response wait time to 0 to disable remote service monitoring.	`0`
`<retries_integer>`	The number of consecutive times remote service monitoring detects a failure before the backup unit changes its effective operating mode to master. The number of times the check fails range is 1 to a very high number. Set the number of times the check fails to 0 to disable remote service monitoring.	`0`

Example

Enter the following command on an active-passive HA backup unit to configure remote services monitoring to monitor the POP3 service on a primary unit interface with IP address 10.10.10.2 using TCP port 110. The command also configures remote service monitoring to check the POP3 service every 30 minutes, wait up to 20 seconds for a response and to change the backup effective operating mode to master if POP3 remote interface monitor fails after 10 consecutive checks.

```
set system ha rservice pop 10.10.10.2 25 30 20 10
```

History

FortiMail v3.0	New.

Related topics

- set system ha config
- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha data
- set system ha datadir
- set system ha lservice
- set system ha mode
- set system ha monitor
- set system ha on-failure
- set system ha passwd
- set system ha remote-as-heartbeat
- set system ha {restart | restore | resync}
- set system ha takeover

system ha takeover

Use this command to configure HA network interface in master mode configuration options for an active-passive HA group to control how network interface IP addressing and status is changed by HA. Depending on your requirements you can configure HA network configuration options for all FortiMail network interfaces; including the `mgmt` interface for a FortiMail unit operating in transparent mode.

For FortiMail units operating in gateway and server modes, for each interface you can ignore the interface, set a new IP address and netmask for the interface, or add a virtual IP and netmask.

For FortiMail units operating in transparent mode you can also configure how the FortiMail management interface (mgmt) configuration is changed by HA. Also in transparent mode you can add individual network interfaces to the FortiMail transparent mode bridge.

Note: Using the `add` option to add a virtual IP address to a FortiMail interface gives the interface two IP addresses: the virtual IP address and the actual IP address. The interface can receive traffic sent to both of these IP addresses. Normally you would configure your network (MX records, firewall policies, routing and so on) so that clients and mail services use the virtual IP address. All replies to sessions with the virtual IP address include the virtual IP address as the source address. All replies to sessions with the actual IP address include the actual IP address as the source address. All outgoing sessions that originate from this interface also use the virtual IP address of the interface and not the actual IP address. This means that all outbound mail or relayed mail packets sent from a FortiMail primary unit interface, configured with a virtual IP address, will have the virtual IP address of the primary unit interface as the source IP address. If you are using this interface to send outgoing email, you should configure your network devices (such as NAT firewalls) to process traffic from the virtual primary unit interface IP address.

Syntax

```
set system ha takeover <interface_str> {add | bridge | ignore | set}
  <takeover_ipv4> <netmask_ipv4>
```

Keywords/Variables	Description	Default
`<interface_str>`	The name of the network interface to configure. For example `port1`, `port2`, `port3`, `mgmt`, and so on depending on your FortiMail unit.	
`{add | bridge | ignore | set}`	Control how the status of the interface is changed by active-passive HA. Enter `add` to assign a virtual IP address to a network interface. `add` corresponds to the web-based manager add virtual IP/netmask option. When operating in HA mode, this option adds the specified IP address to the selected interface of the primary unit. Email processing, FortiMail users, and FortiMail administrators can all connect to this virtual IP address to connect to the primary unit. If a failover occurs, the virtual IP address is transferred to the new primary unit. Email processing, FortiMail users, and FortiMail administrators can now connect to the same IP address to connect to the new primary unit. In most cases you would select add virtual IP/netmask for all FortiMail network interfaces that will be processing email when the FortiMail cluster is operating in gateway or server mode. Enter `bridge`, for a FortiMail HA group operating in transparent mode, for all network interfaces to be added to the FortiMail transparent mode bridge. `bridge` corresponds to the web-based manager add to bridge option. For the primary unit, `bridge` has the same affect as `ignore`. In both cases the interface is added to the bridge. For the backup unit, `bridge` means that the interface is disconnected and cannot process traffic when the effective operating mode of the unit is SLAVE. The interface is disconnected to prevent layer 2 loops. If the effective operating mode of the unit changes to MASTER the interface becomes connected again and as part of the bridge can process traffic. For this reason, `bridge` is the recommended configuration. Enter `ignore` if you do not want to apply special functionality to a network interface when operating in HA mode. `ignore` corresponds to the web-based manager do nothing option. Usually you would leave all FortiMail unit network interfaces that are not connected to your network set to `ignore`. Primary and secondary heartbeat interfaces are automatically set to `ignore` and you should not change this setting. Enter `set` and add an IP address and netmask to change the IP address of the selected network interface of the primary unit to the specified IP address. `set` corresponds to the web-based manager set interface IP/netmask option. When a failover occurs this IP address is assigned to the corresponding network interface of the new primary unit. Changing the IP address of an HA group interface using set interface IP/netmask replaces the actual IP address of the interface with the set IP address. The interface has only one IP address. (This is different from the virtual IP address configuration, which results in the interface having two IP addresses.)	`ignore`

`<takeover_ipv4>`
`<netmask_ipv4>`
	Add an IP address and netmask as required depending on the takeover option that you select. You always have to add an IP address and netmask even if the takeover option does not require one.	`0.0.0.0`
		`0.0.0.0`

Example

Enter the following command to set the port5 interface with a virtual IP address of 10.10.10.2 and a netmask of 255.255.255.0 when the FortiMail unit operates in HA mode.

```
set system ha takeover port5 add 10.10.10.2 255.255.255.0
```

History

FortiMail v3.0	New.

Related topics

- set system ha config
- set system ha {cpeer | interface | peer | secondary-interface | secondary-peer}
- set system ha data
- set system ha datadir
- set system ha lservice
- set system ha mode
- set system ha monitor
- set system ha on-failure
- set system ha passwd
- set system ha remote-as-heartbeat
- set system ha {restart | restore | resync}
- set system ha rservice

system hostname

Use this command to configure the FortiMail unit hostname.

Syntax

```
set system hostname <hostname_str>
```

History

FortiMail v3.0	New.

system interface config

Use this command to configure FortiMail interface access and settings including:

- allowed and denied protocols
- maximum transportation unit (MTU) size
- setting the interface either up or down

Syntax

```
set system interface <intf_str> config allowaccess {ping http https snmp
  ssh telnet} denyaccess {ping http https snmp ssh telnet} mtu <mtu_int>
  speed {auto/10full/10half/100full/100half/1000full} status {down | up}
```

Keywords and Variables	Description
`interface <intf_str>`	Enter the name of the interface or vlan to be configured.
`allowaccess {ping http https snmp ssh telnet}`	Enter the types of management access permitted on this interface or secondary IP address. All types not entered are denied. Enter all required types and separate each type with a space. Items can be removed by re-entering the command with only the required types.
`denyaccess {ping http https snmp ssh telnet}`	Enter the types of management access to be denied on this interface or secondary IP address. The `deny access` command is the equivalent of executing the `allowaccess` command with only the required management access types.
`mtu <mtu_int>`	Enter the maximum transportation unit (MTU) for the specified interface. `<mtu_int>` is the maximum packet size sent from this interface.
`speed {auto/10full/10half/100full/100half/1000full}`	Sets the speed of the network interface. The default is `auto`. Note that some interfaces may not support all speeds.
`status {down | up}`	Sets the specified interface down or up.

History

FortiMail v3.0 New.

Related topics

- set system interface mode dhcp
- set system interface mode dhcp
- set system interface mode static

system interface mode dhcp

Use this command to enable or configure DHCP for this interface.

If only the dhcp keyword is used, both connection and default gateway are enabled by default.

Syntax

To enable DHCP on this interface:

```
set system interface <intf_str> mode dhcp
```

To enable and/or configure DHCP on the interface:

```
set system interface <intf_str> mode dhcp connection {enable | disable}
  defaultgw {enable | disable}
```

Keywords and Variables	Description
`interface <intf_str>`	Enter the name of the interface, `port1`, for example.
`connection {enable | disable}`	Enables or disables connecting to a DHCP server to configure the external interface.
`defaultgw {enable | disable}`	Enables or disables the specified interface to be the default gateway interface.

History

FortiMail v3.0	New.

Related topics

- set system interface config
- set system interface mode static

system interface mode static

Use this command to enable or configure a static IP for this interface.

When setting an interface to static IP mode, an IP address and netmask must be included.

Syntax

```
set system interface <intf_str> mode static ip <addr_ip4> <mask_ip4>
```

History

FortiMail v3.0	New.

Related topics

- set system interface config
- set system interface mode dhcp
- set system route number

system opmode

Use this command to change the operation mode (opmode) of the FortiMail unit.

Only the default FortiMail system administrator account can change the opmode of the FortiMail unit. You will need to login again after changing the opmode.

Changing the opmode between gateway and server modes will result in all settings being changed to factory defaults except the configuration for the port1 interface

Changing the opmode to or from transparent mode will result in all settings being changed back to factory defaults.

Note: It is recommended that you back up the FortiMail configuration before changing the opmode.

Syntax

```
set system opmode {gateway | server | transparent}
```

History

FortiMail v3.0	New.

system option

Use these commands to configure FortiMail administration including:

- timeout on the admin account
- when to start the backend user verification
- web-based manager language
- PIN for the LCD panel
- the refresh interval for the GUI interface

Syntax

```
set system option [ option1 <value1> .. ]
```

The options and their values are as follows:

`admintimeout <timeout_int>`	Use this command to set the idle time-out for system administration. Idle Timeout controls the amount of inactive time that the web-based manager waits before requiring the administrator to log in again. <timeout_int> is the idle timeout number in minutes. The default idle time out is 5 minutes. The maximum idle time out is 480 minutes (8 hours). To improve security, keep the idle timeout at the default value of 5 minutes.
`backend_verify <hh:mm:ss>`	Use this command to set the start time of the backend user verification program. The time is specified in hours (hh), minutes (mm), and seconds (ss). It is in 24 hour format.
`language <language_str>`	Use this command to set the language for the web-based manager to use. <language_str> can be one of english, simplifiedchinese, japanese, korean, or traditionalchinese.
`lcdpin <pin_int>`	Use this command to set the 6 digit personal identification number (PIN) on the FortiMail LCD panel. Once set, the PIN must be entered to make any changes from the front panel. The PIN is only used when lcdprotection is enabled.
`lcdprotection {enable | disable}`	Use this command to turn on the FortiMail front panel LCD password protection. To set the PIN, use the lcdpin keyword.
`refresh {interval | none}`	User this command to set or disable the GUI interface refresh interval.

History

FortiMail v3.0 New.

Related topics

- set system admin
- set system appearance

system route number

Use this command to set and configure system routing.

Syntax

```
set system route number <route_int> dev1 {auto | port1} dst <route_ip4>
  <mask_ip4> gw1 <gway_ip4>
```

Keywords and Variables	Description
`number <route_int>`	Enter the number of the route in the routing table. The default route is 0.
`dev1 {auto | port1}`	Sets the FortiMail traffic-routing interface to auto or port1. In auto, the FortiMail unit routes traffic to the interface that is on the same subnet as gw1.
`dst <route_ip4> <mask_ip4>`	Sets the FortiMail unit route destination IP address and IP address mask. <route_ip4> is the destination IP address. <mask_ip4> is the IP address mask.
`gw1 <gway_ip4>`	Sets the FortiMail unit route primary gateway IP address. <gateway_ipv4> is the primary gateway IP address.

History

FortiMail v3.0	New.

Related topics

- set system interface config
- set system interface mode static

system snmp community

Use this command to set and configure the system simple network management protocol (SNMP) settings.

Syntax

```
set system snmp community number <community_int> config {name <name_str>
  | queryportv1 <port_int> | queryportv2c <port_int> | queryv1_status
  {enable | disable} | queryv2c_status {enable | disable} | status
  {enable | disable} | trapevent {cpu | mem | logdisk | maildisk | deferq
  | virus | spam | system | raid |ha |archive | ipchg | psu} |
  trapportv1_local <port_int>| trapportv1_remote <port_int>|
  trapportv2c_local <port_int>| trapportv2c_remote <port_int>|
  trapv1_status {enable | disable} | trapv2c_status {enable | disable} }
```

Keywords and Variables	Description
`number <community_int>`	Enter the number of this SNMP community.
`name <name_str>`	Enter the name of this SNMP community
`{queryportv1	queryportv2c} <port_int>`	Select the port to listen on for SNMP traffic. The defaults are port 161 for v1 and port 162 for v2c.
`{queryv1_status	queryv2c_status} {enable	disable}`	Activate or deactivate SNMP v1 and v2c traffic.
`status {enable	disable}`	Activate or deactivate this SNMP community.
`trapevent {cpu	mem	logdisk	maildisk	deferq	virus	spam	system	raid	ha	archive	ipchg	psu}`	Select one or more events that will generate a trap when the event occurs or when the threshold is passed. The events are: • cpu - CPU usage threshold • mem - Memory low threshold • logdisk - Logdisk space low threshold • maildisk - Maildisk space low threshold • deferq - Deferred queue threshold • virus - Virus threshold • spam - Spam threshold • system - System component event • raid - RAID system event • ha - HA system event • archive - Remote archive server event • ipchg - Interface IP address changed • psu - Power supply unit (PSU) event System events typically involve a change in state of hardware. To set SNMP trap thresholds, see “set system snmp {sysinfo	threshold}” on page 342.
`{trapportv1_local	trapportv1_remote	trapportv2c_local	trapportv2c_remote } <port_int>`	Select the ports SNMP v1 and v2c use to send traps to SNMP monitors.
`{trapv1_status	trapv2c_status} {enable	disable}`	Activate or deactivate SNMP v1 and v2c traps

Note: The Power Supply Monitored (psu) option for trap event is visible for all FortiMail models. Not all FortiMail models have monitored power supplies.

History

FortiMail v3.0	New.
FortiMail v3.0	Added `psu` to `trapevent` keyword.

Related topics

- set system snmp {sysinfo | threshold}

system snmp {sysinfo | threshold}

Use this command to set and configure SNMP monitoring of the FortiMail unit and thresholds for SNMP traps.

Syntax

```
set system snmp sysinfo status {disable | enable} value <desc_str>
  <loc_dtr> <contact_str>
set system snmp threshold {cpu | deferq | logdisk | maildisk | mem | spam
  |virus } <trigger_int>
```

Keywords and Variables	Description
`status {disable | enable}`	Activate or deactivate SNMP monitoring of the FortiGate unit.
`value <desc_str> <loc_str> <contact_str>`	Set the description and contact information associated with this FortiMail unit. When an SNMP manager receives information from this FortiMail unit, this description will help determine which unit is which. If the string includes spaces, enclose the string in quotes. <desc_str> is the unique description of this unit. <loc_str> is the location of this unit. <contact_str> is the contact information for the administrator for this unit
`threshold {cpu | deferq | logdisk | maildisk | mem | spam |virus } <trigger_int>`	Set the threshold for one of the SNMP traps. Trigger sets a threshold value between 1 and 99 that will trigger that trap. The thresholds are for the following SNMP traps: • cpu - CPU usage - Percentage of CPU used (default is 80%) • deferq - High deferred mail queue - Disk space used for deferred queue (default is 1000) • logdisk - Log disk usage - Log disk percentage full (default is 90%) • maildisk - Mail Disk usage - Mail disk percentage full (default is 90%) • mem - Memory low - Percentage of memory in use (default is 80%) • spam - Detected spam - Number of spam detections (default is 1) • virus - Detected viruses - Number of virus detections (default is 1) For example if maildisk has a trigger of 75, when the hard disk is 75% filled up it will trigger the maildisk SNMP trap. Another example is if virus has a trigger of 4, when 4 viruses are detected it will trigger the virus SNMP trap.

History

FortiMail v3.0	New.

Related topics

- set system snmp community

system time manual

Use this command to set and configure system time settings manually.

Syntax

```
set system time manual clock <hh:mm:ss> date <mm/dd/yyyy> dst {disable |
  enable} zone <zone_num>
```

Keywords and Variables	Description
`clock <hh:mm:ss>`	Enter the system time by hour, minute, and second.
`date <mm/dd/yyyy>`	Enter the system time by month, day, and year.
`dst` `{disable	enable}`	Enable or disable daylight saving time (DST).
`zone <zone_num>`	Enter the time zone, by number, the FortiMail unit is . Use '?' to see a list of zone names and their numbers.

History

FortiMail v3.0 New.

Related topics

- set system time ntp

system time ntp

Use this command to set and configure system time settings using network time protocol (NTP).

Syntax

```
set system time ntp dst {disable | enable} ntpserver <ipv4 | hostname>
  ntpsync {disable | enable} syncinterval <sync_interval> zone <zone_num>
```

Keywords and Variables	Description
`dst {disable | enable}`	Enable or disable daylight saving time (DST).
`ntpserver <ipv4 | hostname>`	Enters NTP server IP or hostname. • <ipv4> is the NTP server IP address. • <hostname> is the NTP server hostname
`ntpsync {disable | enable}`	Enable to synchronize the FortiMail unit with the NTP server.
`syncinterval <sync_interval>`	Enter the system synchronization time interval from one to 1440 minutes.
`zone <zone_num>`	Enter the required time zone by number. Use ‘?’ to see a list of zone names and their numbers.

History

FortiMail v3.0 New.

Related topics

- set system time manual

system usrgrp

Use this command to add a user group and its members to the specified domain.

Syntax

```
set system usrgrp domain <domain> name <'usrgrp_name_str'> member
  <'usrgrp_name_str' .. >
```

Keywords and Variables	Description
`domain <domain>`	Enter the domain where you are adding a usergroup.
`name <'usrgrp_name_str'>`	Enter the name of the new usergroup. Enclose it in quotes
`member <'usrgrp_name_str' .. >`	Enter the name or names of the members of this new usergroup. One or more names are required. Multiple users are added after the member keyword, with each user in single quotes.

Example

For the domain example.com, the users called user1, and user3 will be added to a group called test. This domain and these users must exist before entering this command.

```
set system usrgrp domain example.com name ‘test’ member ‘user1’ ‘user3’
```

History

FortiMail v3.0	New.

Related topics

- set system admin
- set user

user

Use this command to configure email users, user groups, and user aliases in server mode.

Arguments must be in valid email format.

Syntax

To set up the alias:

```
set user alias name <name_str> member '<addr> [<addr>...]'
```

To add new members to the alias

```
set user alias name <name_str> add_member '<addr> [<addr>...]'
```

To map a user to another email address:

```
set user map internal_name <int_str> external_name <ext_str>
```

To map LDAP aliased users to a domain:

```
set user ldap map domain <domain_name> profile <ldapprofile_name>
```

Commands	Description	Default
`alias name <name_str>`	`<name_str>` is the email alias address.	
`add_member '<addr> [<addr>...]'`	Add new members to the specified alias. `<addr>` are the email addresses of member to be added to the alias.	
`member '<addr> [<addr>...]'`	Enter the user alias name and members for this alias. Any previously existing members in the list not specified in this command are deleted from the list. `<addr>` is the email address of a member.	
`map internal_name <int_str> external_name <ext_str>`	Enter a user map for an email address. • `<int_str>` is the user's actual email address. • `<ext_str>` is the address that will be remapped to the user's actual email address.	

History

FortiMail v3.0	New.

user pki

Use this command to configure PKI authentication for users.

Syntax

```
set user pki name <name_str> ca <cert_str>
set user pki name <name_str> domain <domain_str>
set user pki name <name_str> ldapfield {subject alternative | cn}
set user pki name <name_str> ldapprofile <profile_str>
set user pki name <name_str> ldapquery {enable | disable}
set user pki name <name_str> ocspaction {revoke | ignore}
set user pki name <name_str> ocspca <url>
set user pki name <name_str> ocspverify {enable | disable}
set user pki name <name_str> subject <subject_str>
```

Commands	Description	Default
`<name_str>`	`<name_str>` is the PKI user name.	
`ca <cert_str>`	Enter the name of the CA certificate used when validating the CA's signature of the client certificate.	
`domain <domain_str>`	Enter the protected domain to which the PKI user is assigned. If Domain is System, the PKI user belongs to all domains configured on the FortiMail unit.	
`ldapfield {subject alternative | cn}`	Enter the name of the field in the client certificate (either CN or Subject Alternative) which contains the email address of the PKI user.	
`ldapprofile <profile_str>`	Enter the LDAP profile to use when querying the LDAP server.	
`ldapquery {enable | disable}`	Enable to query an LDAP directory, such as Microsoft ActiveDirectory, to determine the existence of the PKI user who is attempting to authenticate, then also configure LDAP Profile and Query Field.	
`ocspaction {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.	
`ocspca <url>`	The URL of the OCSP server.	
`ocspverify {enable | disable}`	Enable to use an Online Certificate Status Protocol (OCSP) server to query whether the client certificate has been revoked.	
`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 v3.0 MR4 New.

userpolicy delete

Use this command to delete the specified user policy. This command applies to server mode only.

Syntax

```
set userpolicy <name_str> delete
```

`<name_str>` is the name of the policy, expressed with the domain. For example, user34@example.com and *@example.com are both valid policy names.

History

FortiMail v3.0	New.

Related topics

- set userpolicy move-to
- set userpolicy rename-to

userpolicy modify

Use this command to define the profiles used with the specified policy. This command applies to server mode only.

Syntax

```
set userpolicy <name_str> modify as <as_str> av <av_str> misc <misc_str>
  content <content_str>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the policy, expressed with the domain.	
`<as_str>`	Enter the name of the antispam profile to use with this policy.	`antispam_def`
`<av_str>`	Enter the name of the antivirus profile to use with this policy.	`antivirus_def`
`<misc_str>`	Enter the name of the misc profile to use with this policy.	`misc_def`
`<content_str>`	Enter the name of the content profile to use with this policy.	`content_def`

History

FortiMail v3.0	New.

Related topics

- set userpolicy delete
- set userpolicy move-to
- set userpolicy rename-to

userpolicy move-to

Use this command to move the specified policy to a new position in the policy list. This command applies to server mode only.

Syntax

```
set userpolicy <name_str> move-to <new_int>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the policy, expressed with the domain.	
`<new_int>`	Enter the number value of the new position in the list.	

History

FortiMail v3.0	New.

Related topics

- set userpolicy delete
- set userpolicy rename-to

userpolicy rename-to

Use this command to rename an existing user policy. This command applies to server mode only.

Syntax

```
set userpolicy <name_str> rename-to <new_str>
```

Keywords and Variables	Description	Default
`<name_str>`	This is the name of the policy, expressed with the domain.	
`<new_str>`	Enter the new name of the specified policy.	

History

FortiMail v3.0	New.

Related topics

- set userpolicy delete
- set userpolicy move-to

unset

This chapter describes the following commands:

alertemail configuration

Use this command to remove the alertemail configuration.

Syntax

```
unset alertemail configuration
```

History

FortiMail v3.0	New.

ldap_profile

Use this command to delete an LDAP profile.

Syntax

```
   unset ldap_profile profile <name_str>
```

`<name_str>` is the name of the LDAP profile to delete.

History

FortiMail v3.0	New.

log reportconfig

Use this command to delete a log configuration.

Syntax

```
unset log reportconfig <name_str>
```

`<name_str>` is the name of the log configuration.

History

FortiMail v3.0	New.

mailserver

Use this command to remove parts of the email server configuration.

Syntax

```
unset mailserver <configuration>
```

`<configuration>`	**Description**
`access domain <domain_str>`	Remove the email server access permissions to and from the specified domain.
`archiveexempt id <id_value>`	Remove an archiving exempt policy based on the policy ID entered.
`archivepolicy id <id_value>`	Remove an archiving policy based on the policy ID entered.
`localdomain <string>`	Remove the specified local domain. (Server mode only).
`smtp clientconn exempt <exempt_str>`	Enter the IP address that you wish to exclude from connection number control.
`smtp clientrate exempt <exempt_str>`	Enter the IP address that you wish to exclude from connection rate control.

History

FortiMail v3.0	New.

system

Use this command to remove parts of the system configuration.

Syntax

```
unset system <configuration>
```

`<configuration>`	Description
`admin username <account_str>`	Delete the configured administrator account. <account_str> - the name of the administrator account
`ddns server <server_str> domain <domain_str>`	Reset the dynamic domain name service (DDNS) server settings to factory default. <server_str> - the name of the DDNS service <domain_str> - the name of the DDNS hosted domain
`hostname`	Set the FortiMail unit's name to "" (blank).
`localdomainname`	Set the local domain name to "" (blank).
`route number <route_int>`	Clear the route entry. <route_int> - entry in the routing table
`snmp comm_host number <community_int> <host_int>`	Clear the SNMP community host. <community_int> - the index of the configured community <host_int> - the index of the configured host
`snmp community number <community_int>`	Reset the SNMP community. <community_int> - the index of the configured community
`usrgrp domain <domain_int> name 'usrgrp_name'`	Reset specified user group for the specified domain to blank. <domain_int> is the number of the configured domain. 'usrgrp_name' is the name of the user group.

History

FortiMail v3.0 MR3 New.

user (transparent and gateway)

Use this command to remove parts of the user configuration.

Syntax

```
unset user <configuration>
```

`<configuration>`	Description
`alias name <alias_str>`	Delete this user alias. <alias_str> - the name of the alias
`map name <map_str>`	Delete this user map. <map_str> - the name of the user map

History

FortiMail v3.0 MR3 New.

Related topics

-
-

user (server)

Use this command to remove parts of the user configuration.

Syntax

```
unset user <configuration>
```

`<configuration>`	**Description**
`alias name <alias_str>`	Delete this user alias. <alias_str> - the name of the user alias
`group name <group_str>`	Delete this group. <group_str> - the name of the user group
`ldap map domain <domain_int>`	Delete the mapping between the domain and the profile. <domain_int> - the name of the domain associated with the LDAP mapping
`map name <map_str>`	Delete this user map. <map_str> - the name of the user map

History

FortiMail v3.0 MR3 New.

Index

www.fortinet.com

FORTINET™

www.fortinet.com