CLI Reference

FortiMail 7.6.2

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 18, 2026
FortiMail 7.6.2 CLI Reference
06-762-000000-20260218

TABLE OF CONTENTS

Change log

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

Date	Change Description
2024-12-04	Initial release of the FortiMail 7.6.2 CLI Reference.
2025-06-04	Fix to mailsetting relay-host-list on page 130 to clarify the load balancing algorithm of each relay type.
2026-01-30	Fix to restore the missing setting smtp-smtputf8 {enable | disable} on page 336.
2026-02-10	Fix to profile antispam on page 167 to remove old setting names for sender alignment, and to placement of business email compromise (BEC) dependencies and description.

Using the CLI

The command line interface (CLI) is an alternative to the web user interface (GUI).

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

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

Connecting to the CLI

You can access the CLI in two ways:

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

Local access is required in some cases.

If you are installing your FortiMail unit for the first time and it is not yet configured to connect to your network, unless you reconfigure your computer's network settings for a peer connection, you may only be able to connect to the CLI using a local serial console connection.

Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until **after** the boot process has completed, and therefore local CLI access is the only viable option.

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

This section includes:

Local console connection and initial configuration

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

Requirements

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

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

To connect to the CLI using a local serial console connection

1. Using the null modem or RJ-45-to-DB-9 cable, connect the FortiMail unit's console port to the serial communications (COM) port on your management computer.
2. On your management computer, start PuTTY.
3. In the **Category** tree on the left, go to **Connection > Serial** and configure the following:

Serial line to connect to	COM1 (or, if your computer has multiple serial ports, the name of the connected serial port)
Speed (baud)	9600
Data bits	8
Stop bits	1
Parity	None
Flow control	None

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

```
Welcome!
```

Initial configurations

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

To change the admin password:

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

```
end
```

To change the operation mode:

```
config system global
   set operation-mode {gateway | server | transparent}
end
```

To configure the interface IP address:

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

To configure the system route/gateway:

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

To configure the DNS servers:

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

To configure the NTP time synchronization:

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

To configure the SNMP v3 user settings:

```
config system snmp user
   edit <user_name>
      set query-status {enable | disable}
      set queryport <port_number>
      set security-level {authnopriv | authpriv | noauthnopriv}
      set auth-proto {sha1 | md5}
      set auth-pwd <password>
      set status {enable | disable}
      set trap-status {enable | disable}
      set trapevent {cpu | deferred-queue | ha | ip-change | logdisk | maildisk | mem | raid |
            remote-storage | spam | system | virus}
      set trapport-local <port_number>
      set trapport-remote <port_number>
   config host
```

```
      edit <host_no>
         set ip <class_ip>
   end
end
```

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

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

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

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

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

You can do this using either:

- a local console connection
- the web manager

Requirements

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

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

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

Note the number of the physical network port.

Using a local console connection, connect and log into the CLI. For details, see Local console connection and initial configuration on page 18.

Enter the following commands:

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

where:

`<interface_str>` is the name of the network interface associated with the physical network port, such as `port1`

Enter the administrative access protocols you wish to permit in a space-delimited format, such as `https ssh telnet`; omit protocols that you do not want to permit.

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

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

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

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

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

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

To connect to the CLI through the network interface, see Connecting to the CLI using SSH on page 22 or Connecting to the CLI using Telnet on page 23.

Connecting to the CLI using SSH

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

SSH provides both secure authentication and secure communications to the CLI. Supported SSH protocol versions, ciphers, and bit strengths vary by whether or not you have enabled FIPS-CC mode, but generally include SSH version 2 with AES-128, 3DES, Blowfish, and SHA-1.

Requirements

- a FortiMail network interface configured to accept SSH connections (see Enabling access to the CLI through the network (SSH or Telnet) on page 21)
- terminal emulation software such as PuTTY

To connect to the CLI using SSH

1. On your management computer, start PuTTY.
2. In **Host Name (or IP Address)**, type the IP address of a network interface on which you have enabled SSH administrative access.
3. In **Port**, type 22.
4. From **Connection type**, select **SSH**.
5. Click **Open**.
   The SSH client connects to the FortiMail unit.
   The SSH client may display a warning if this is the first time you are connecting to the FortiMail unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiMail unit but it used a different IP address or SSH key. If your management computer is directly connected to the FortiMail unit with no network hosts between them, this is normal.
6. Click **Yes** to verify the fingerprint and accept the FortiMail unit's SSH key. You will not be able to log in until you have accepted the key.
   The CLI displays a login prompt.
7. Type a valid administrator account name (such as `admin`) and press **Enter**.

You can alternatively log in using an SSH key. For details, see system admin on page 275.

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

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

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

Connecting to the CLI using Telnet

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

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

Requirements

- a FortiMail network interface configured to accept Telnet connections (see Enabling access to the CLI through the network (SSH or Telnet) on page 21)
- terminal emulation software such as PuTTY

To connect to the CLI using Telnet

1. On your management computer, start PuTTY.
2. In **Host Name (or IP Address)**, type the IP address of a network interface on which you have enabled Telnet administrative access.
3. In **Port**, type `23`.
4. From **Connection type**, select **Telnet**.
5. Click **Open**.
   The CLI displays a login prompt.
6. Type a valid administrator account name (such as `admin`) and press **Enter**.
7. Type the password for this administrator account and press **Enter**.

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

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

Logging out from the CLI console

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

Command syntax

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

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

See also

Using the CLI

Terminology

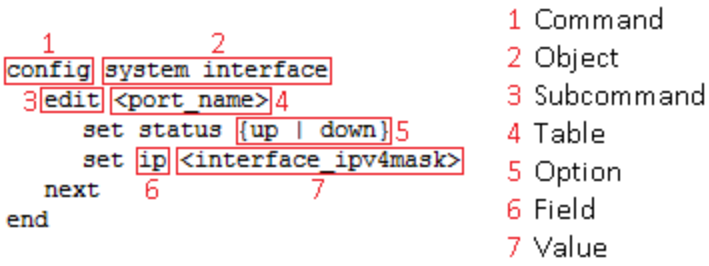
Each command line consists of a command word that is usually followed by words for the configuration data or other specific item that the command uses or affects:

```
get system admin
```

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

```
config system interface
   edit <port_name>
      set status {up | down|
      set ip <interface_ipv4mask>
   next
end
```

Command syntax terminology:



- **Command** — A word that begins the command line and indicates an action that the FortiMail unit should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that end when you press the Enter key, it forms a command line. Exceptions include multi-line command lines, which can be entered using an escape sequence (See Shortcuts and key commands on page 36).

  Valid command lines must be unambiguous if abbreviated (see Command abbreviation on page 36). Optional words or other command line permutations are indicated by syntax notation (See Notation on page 26).

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

- **Object** — A part of the configuration that contains tables and/or fields. Valid command lines must be specific enough to indicate an individual object.
- **Subcommand** — A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command. Indentation is used to indicate levels of nested commands (See Indentation on page 26).

  Not all top-level commands have sub-commands. Available sub-commands vary by their containing scope (See Sub-commands on page 28).
- **Table** — A set of fields that is one of possibly multiple similar sets which each have a name or number, such as an administrator account, policy, or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them (See Notation on page 26).
- **Option** — A kind of value that must be one or more words from of a fixed set of options (See Notation on page 26).
- **Field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiMail unit will discard the invalid table.

- **Value** — A number, letter, IP address, or other type of input that is usually your configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation (See Notation on page 26).

Indentation

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

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

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

For information about available sub-commands, see Sub-commands on page 28.

See also

Terminology

Notation

Notation

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

Command syntax notation:

Convention	Description

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

Angle brackets `< >`	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: `<retries_int>` indicates that you must enter a number of retries, such as `5`. Data types include: • `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`.

Convention	Description
	• <xxx_index>: An index number referring to another part of the configuration, such as 0 for the first static route. • <xxx_pattern>: A regular expression or word with wild cards that matches possible variations, such as the regular expression .*@example\.com to match all email addresses ending in @example.com. For examples and details about regular expression and wild cards, see the FortiMail Administration Guide. • <xxx_fqdn>: A fully qualified domain name (FQDN), such as mail.example.com. • <xxx_email>: An email address, such as admin@mail.example.com. • <xxx_url>: A uniform resource locator (URL) with the protocol, host name, possibly the port number, and page or API, such https://docs.fortinet.com/document/fortimail/7.6.2/cli-reference/991136/sub-commands. • <xxx_ipv4>: An IPv4 address, such as 192.168.1.99. • <xxx_v4mask>: A dotted decimal IPv4 netmask, such as 255.255.255.0. • <xxx_ipv4mask>: A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0. • <xxx_ipv4/mask>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as 192.168.1.99/24. • <xxx_ipv4range>: A hyphen (-) delimited inclusive range of IPv4 addresses, such as 192.168.1.1-192.168.1.255. • <xxx_ipv6>: A colon (:) delimited hexadecimal IPv6 address, such as 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234. • <xxx_v6mask>: An IPv6 netmask, such as /96. • <xxx_ipv6mask>: An IPv6 address and netmask separated by a space. • <xxx_str>: A string of characters that is **not** another data type, such as P@ssw0rd. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See Special characters on page 37. • <xxx_float>: A decimal number that is **not** another data type, such as 10.000000 for a threshold. • <xxx_int>: An integer number that is **not** another data type, such as 15 for the number of minutes.
Curly braces { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].
Options delimited by vertical bars |	Mutually exclusive options. For example: {enable | disable} indicates that you must enter either enable or disable, but must not enter both.
Options delimited by spaces	Non-mutually exclusive options. For example: {http https ping snmp ssh telnet} indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: ping https ssh

Convention	Description
	Note: To change the options, you must re-type the entire list. For example, to add `snmp` to the previous example, you would type: `ping https snmp ssh` If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

See also

Indentation

Terminology

Sub-commands

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

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

```
get system admin
```

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

```
config system admin
```

the command prompt becomes:

```
(admin)#
```

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

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

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

Sub-command scope is indicated in this guide by indentation. See Indentation on page 26.

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

- commands affecting fields
- commands affecting tables

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

Commands for tables:

`delete <table_name>`	Remove a table from the current object. For example, in `config system admin`, you could delete an administrator account named `newadmin` by typing `delete newadmin` and pressing Enter. This deletes `newadmin` and all its fields, such as `newadmin`'s `name` and `email-address`. `delete` is only available within objects containing tables.
`edit <table_name>`	Create or edit a table in the current object. For example, in `config system admin`: • edit the settings for the default `admin` administrator account by typing `edit admin`. • add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`. `edit` is an interactive sub-command: further sub-commands are available from within `edit`. `edit` changes the prompt to reflect the table you are currently editing. `edit` is only available within objects containing tables.
`end`	Save the changes to the current object and exit the `config` command. This returns you to the top-level command prompt.
`get`	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values. **Tip:** To get the default value (regardless of its current configuration), see View a setting's default value on page 39.
`purge`	Remove all tables in the current object. For example, in `config forensic user`, you could type `get` to see the list of user names, then type `purge` and then `y` to confirm that you want to delete all users. `purge` is only available for objects containing tables. **Caution:** Back up the FortiMail unit before performing a `purge`. `purge` cannot be undone. To restore purged tables, the configuration must be restored from a backup. For details, see backup on page 367. **Caution:** Do not purge `system interface` or `system admin` tables. `purge` does not provide default tables. This can result in being unable to connect or log in, requiring the FortiMail unit to be formatted and restored.
`rename <table_name> to <table_name>`	Rename a table. For example, in `config system admin`, you could rename `admin3` to `fwadmin` by typing `rename admin3 to fwadmin.` `rename` is only available within objects containing tables.
`show`	Display changes to the default configuration. Changes are listed in the form of configuration commands.

Example of table commands:

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

```
edit admin_1
```

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

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

Commands for fields:

`abort`	Exit both the `edit` and/or `config` commands without saving the fields.

`chattr`	Show which of the command's attributes are synchronized for HA. Use the `sync-disable` and `sync-unset` subcommands to change the attributes (`chattr`) that you wish to be synchronized across HA cluster members.
	  Only administrators with `super_admin` privileges may configure the feature on the primary HA unit.
	To define HA attribute synchronization, configure the following:
	`config <command>`
	`chattr sync-disable ...`
	`chattr sync-unset ...`
	`end`
	Use `chattr sync-disable` to disable any attributes from being synchronized across the HA cluster.
	Use `chattr sync-unset` to reset the attribute's default synchronization behavior.
	You can also enter `chattr` without an argument within a `config` command to display all attributes that can be configured for HA attribute synchronization.
	Additionally, you can use the following `diagnose` commands:
	• `diagnose system ha show-sync-disable-cfg`
	Display all attributes that have been modified or disabled by the administrator.
	• `diagnose system ha show-sync-disable-cfg all`
	Display all attributes that are not synchronized, including both system default and settings disabled by the administrator.
	• `diagnose system ha unset-sync-disable-cfg`
	Enter this command on both primary and secondary units to change all modified or disabled attributes to the default synchronize action.
	Note: If you only enter the command on one of the units, it will cause desynchronization between the cluster members.

`end`	Save the changes made to the current table or object fields, and exit the `config` command (to exit without saving, use `abort` instead).
`get`	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values.

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

Example of field commands:

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

```
set passwd my1stExamplePassword
```

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

Permissions

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

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

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

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

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

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

- **System > Maintenance**
- **Monitor** except for the **Personal quarantine** tab
- **System** except for the **Administrator** tab
- **System > Mail Settings** except for the domain, its subdomains, and associated domains
- **Domain & User > User > PKI User**
- **Policy > Access Control > Receiving**
- **Policy > Access Control > Delivery**
- **Profile > Authentication**
- **Profile > AntiSpam**
- **Email Archiving**
- **Log & Report**

Access profiles assign either read, write, or no access to each area of the FortiMail software. To view configurations, you must have read access. To make changes, you must have write access. For more information on configuring an access profile that administrator accounts can use, see sensitive data on page 272.

These are the possible permission types for an administrator account:

- **Administrator** (also known as **all**)
- **Read & Write**
- **Read Only**

Administrator account permissions by domain assignment:

Permission	Domain: system	Domain: example.com
Administrator	• Can create, view and change all other administrator accounts except the `admin` administrator account • Can view and change all parts of the FortiMail unit's configuration, including uploading configuration backup files and restoring firmware default settings. • Can release and delete quarantined email messages for all protected domains. • Can back up and restore	• Can create, view and change other administrator accounts with **Read & Write** and **Read Only** permissions in its own protected domain. • Can only view and change settings, including profiles and policies, in its own protected domain. • Can only view profiles and policies created by an administrator whose **Domain** is **system**. • Can be only one per protected domain.

Permission	Domain: system	Domain: example.com
	databases. • Can manually update firmware and antivirus definitions. • Can restart and shut down the FortiMail unit.	
Read & Write	• Can only view and change its own administrator account. • Can view and change parts of the FortiMail unit's configuration at the system and protected domain levels. • Can release and delete quarantined email messages for all protected domains. • Can back up and restore databases.	• Can only view and change its own administrator account. • Can only view and change parts of the FortiMail unit's configuration in its own protected domain. • Can only view profiles and policies created by an administrator whose **Domain** is **system.** • Can release and delete quarantined email messages in its own protected domain.
Read Only	• Can only view and change its own administrator account. • Can view the FortiMail unit configuration at the system and protected domain levels • Can release and delete quarantined email messages for all protected domains. • Can back up databases.	• Can only view and change its own administrator account. • Can only view settings in its own protected domain. • Can only view profiles and policies created by an administrator whose **Domain** is **system**.

Areas of control in access profiles:

Access control area name		Grants access to...
In the GUI	**In the CLI**	For each `config` command, there is an equivalent `get/show` command, unless otherwise noted. `config` access requires write permission. `get/show` access requires read permission.
Policy	`policy`	**Monitor > Mail Queue ...** **Monitor > Greylist ...** **Monitor > Reputation > Sender Reputation** **Domain & User > Domain > Domain** **System > Mail Setting > Proxies** **Domain & User > User ...** **Policy ...** **Profile ...** **AntiSpam > Greylist ...** **AntiSpam > Bounce Verification > Settings**

Access control area name		Grants access to...
In the GUI	**In the CLI**	For each `config` command, there is an equivalent `get`/`show` command, unless otherwise noted. `config` access requires write permission. `get`/`show` access requires read permission.
		AntiSpam > Endpoint Reputation ... **AntiSpam > Bayesian ...**

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

Block/Safelist	`block-safe-list`	**Monitor > Endpoint Reputation > Auto blocklist** **Maintenance > AntiSpam > Block/Safelist Maintenance** **AntiSpam > Block/Safelist ...**

		`N/A`
		`diagnose ...`
		`execute ...`
		`get system status`
		`get system raid-performance`
		`get system performance`

Quarantine	`quarantine`	**Monitor > Quarantine ...** **AntiSpam > Quarantine > Quarantine Report** **AntiSpam > Quarantine > System Quarantine Setting** **AntiSpam > Quarantine > Control Account**

		`diagnose ...`
		`execute ...`
		`config antispam quarantine-report`
		`config mailsetting systemquarantine`

Others	`others`	**Monitor > System Status ...** **Monitor > Archive > Email Archives** **Monitor > Log ...** **Monitor > Report ...** **Maintenance** ... **except** the **Block/Safelist Maintenance** tab **System** ... **Mail Settings > Settings** ... **Mail Settings > Address Book > Address Book**

Access control area name		Grants access to...
In the GUI	In the CLI	For each `config` command, there is an equivalent `get`/`show` command, unless otherwise noted. `config` access requires write permission. `get`/`show` access requires read permission.
		User > User Alias > User Alias **User > Address Map > Address Map** **Email Archiving** ... **Log and Report** ...

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

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

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

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

Tips and tricks

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

Help

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

Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.

Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

Shortcuts and key commands

Action	Keys
List valid word completions or subsequent words. If multiple words could complete your entry, display all possible completions with helpful descriptions of each.	?
Complete the word with the next available match. Press the key multiple times to cycle through available matches.	Tab
Recall the previous command. Command memory is limited to the current session.	Up arrow, or Ctrl + P
Recall the next command.	Down arrow, or Ctrl + N
Move the cursor left or right within the command line.	Left or Right arrow
Move the cursor to the beginning of the command line.	Ctrl + A
Move the cursor to the end of the command line.	Ctrl + E
Move the cursor backwards one word.	Ctrl + B
Move the cursor forwards one word.	Ctrl + F
Delete the current character.	Ctrl + D
Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as `config` or `edit`, this closes the CLI connection.	Ctrl + C
Continue typing a command on the next line for a multi-line command. For each line that you want to continue, terminate it with a backslash (\ ). To complete the command line, terminate it by pressing the spacebar and then the Enter key, without an immediately preceding backslash.	\ then Enter

Command abbreviation

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

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

Environment variables

The CLI supports the following environment variables. Variable names are case-sensitive.

$USERFROM	The management access type (`ssh`, `telnet`, `jsconsole` for the **CLI Console** widget and so on) and the IP address of the administrator that configured the item.
$USERNAME	The account name of the administrator that configured the item.
$SerialNum	The serial number of the FortiMail unit.

For example, the FortiMail unit's host name can be set to its serial number.

```
config system global
   set hostname $SerialNum
end
```

As another example, you could log in as `admin1`, then configure a restricted secondary administrator account for yourself named `admin2`, whose `first-name` is `admin1` to indicate that it is another of your accounts:

```
config system admin
   edit admin2
      set first-name $USERNAME
```

Special characters

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

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

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

Character	Keys
(to be interpreted as part of a string value, not to end the string)	
\	\\

Language support

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

For example, the host name must not contain special characters, and so the GUI and CLI will not accept most symbols and non-ASCII encoded characters as input when configuring the host name. This means that languages other than English often are not supported. However, some configuration items, such as names and comments, may be able to use the language of your choice. But dictionary profiles support terms encoded in UTF-8, and therefore support a number of languages.

In addition, names of items in the configuration entered using non-ASCII encodings may not display correctly in event log messages.

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

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

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

Screen paging

You can configure the CLI to, when displaying multiple pages' worth of output, pause after displaying each page's worth of text. When the display pauses, the last line displays `--More--`. You can then either:

- Press the spacebar key to display the next page.
- Type `Q` to truncate the output and return to the command prompt.

This may be useful when displaying lengthy output, such as the list of possible matching commands for command completion, or a long list of settings. Rather than scrolling through or possibly exceeding the buffer of your terminal emulator, you can simply display one page at a time.

To configure the CLI display to pause when the screen is full:

```
config system console
   set output more
end
```

Baud rate

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

Editing the configuration file on an external host

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

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

To edit the configuration on your computer:

1. Use backup to download the configuration file to a TFTP server, such as your management computer.
2. Edit the configuration file using a plain text editor that supports Unix-style (`LF` only, not `CR LF`)line endings.

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

3. Use restore config to upload the modified configuration file back to the FortiMail unit.
   The FortiMail unit downloads the configuration file and checks that the model information is correct. If it is, the FortiMail unit loads the configuration file and checks each command for errors. If a command is invalid, the FortiMail unit ignores the command. If the configuration file is valid, the FortiMail unit restarts and loads the new configuration.

View a setting's default value

You can use the `get default-value` command to view the default value of any objects, table, or settings, from anywhere in the CLI.

This can be especially useful since default values may vary depending upon other prerequisite commands, which FortiMail firmware version you are running, and which FortiMail model you have. You also may not want to

or may not have permissions to use the `unset` command in order to see the default value of a field, because it changes the configuration.

For example, the following command shows the default values of settings in `config system admin`:

```
# get default-value system admin
System Time: 2023-08-17 09:07:28 PDT (Uptime: 1d 2h 5m)
access : cli gui rest
access-profile :
auth-strategy : local
language :
level : system
password : *
ssh-certificate :
sshkey :
status : enable
theme : Green
trusted-hosts : 0.0.0.0/0 ::/0
webmode : simple
wildcard : disable
```

config

`config` commands configure your FortiMail settings.

This chapter describes the following `config` commands:

antispam behavior-analysis

Use this command to analyze the similarity of uncertain email against those well-known spam messages which are received recently.

Syntax

```
config antispam behavior-analysis
   set status {enable | disable}
   set analysis-level{high |  medium |  low}
end
```

Variable	Description	Default
status {enable | disable}	Enable or disable behavior analysis service.	enable
analysis-level {high | medium | low}	Enter the analysis level.	medium

Related topics

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

antispam bounce-verification

Use this command to configure bounce address tagging and verification.

Syntax

```
config antispam bounce-verification ...
   key
   tag-exempt-list
   verify-exempt-list
end
```

Variable	Description	Default
key	Enter a new or existing key.	
tag-exempt-list	Exempt domain list for BATV tagging.	
verify-exempt-list	Exempt host name of reverse DNS lookup of sending IP for BATB verification.	

Related topics

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

antispam deepheader-analysis

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

Deep header analysis examines the entire message header for spam characteristics.

Not all headers may be checked, depending on your configuration of antispam trusted on page 60.

Syntax

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

Variable	Description	Default
confidence <percent_float>	Type the confidence percentage above which a message will be considered spam. The deep header scan examines each message and calculates a confidence value based on the results of the decision-tree analysis. The higher the calculated confidence value, the more likely the message is considered spam. The deep header scan adds an `X-FEAS-DEEPHEADER:` line to the message header that includes the message's calculated confidence value.	95.000000
greyscale-level <level_int>	Type the grey scale threshold above which the deep header scan will be skipped. FortiGuard AntiSpam service uses the scale of 1-9 to determine the certainty of an email being spam. 1-4 means the email is almost definitely spam, while 9 is not. Increasing this threshold increases the probability of catching all spam, but can also increase false positives.	7

Related topics

profile antispam
antispam trusted
antispam greylist exempt
antispam settings

antispam dmarc-report-generation

Use this command to configure system-level settings for Domain-based Message Authentication, Reporting & Conformance (DMARC) reports. Administrators may use these reports to determine the effectiveness of their DMARC policies.

Syntax

```
config antispam dmarc-report-generation
   set status {enable | disable | monitor-only}
   set max-num-of-to-domain <maximum_int>
   set from-addr-localpart <localpart_str>
end
```

Variable	Description	Default
status {enable | disable | monitor-only}	Select either: • `enable`:Collect DMARC check data. Each day, for each sender domain that matched a policy where DMARC checks are enabled, send a report to that domain's authorized DMARC report recipient. **Note:** If a sender does not have a valid DMARC RUA/RUF configured in the domain's DNS TXT record, then even if you enable DMARC reports, FortiMail cannot send them to that domain because there is no report recipient email address. **Tip:** If you have the DMARC report analysis feature license, then you can instead use charts with statistics about DMARC reports.You can also generate DMARC reports on demand, and send them to other recipients. See dmarc-report-analysis-status {enable | disable}. • `disable`: Do not collect DMARC check data. Do not generate a report. • `monitor-only`: Collect DMARC check data, but do not generate a report.	disable
max-num-of-to-domain <maximum_int>	Enter the maximum number of sender domains that FortiMail will send DMARC reports to per day. Valid range varies by your FortiMail platform. See FortiMail Maximum Values.	100
from-addr-localpart <localpart_str>	Enter the local part (username) that the FortiMail unit will use as its sender email address (`From:`) when it sends DMARC report email. Change it if, for example, an administrator wants replies about this DMARC report.	noreply

Related topics

antispam settings

domain-setting

profile antispam

system advanced-management

antispam endpoint reputation blocklist

Use this command to manually blocklist carrier end points by MSISDN.

MSISDN numbers listed on the blocklist will have their email or text messages blocked as long as their identifier appears on the blocklist.

Syntax

```
config antispam endpoint reputation blocklist
   edit <msisdn>
end
```

Variable	Description	Default
<msisdn>	Type the MSISDN number to blocklist carrier end point.	

Related topics

profile antispam

antispam trusted

antispam endpoint reputation exempt

Use this command to manually exempt carrier end points by MSISDN from automatic blocklisting due to their endpoint reputation score.

Syntax

```
config antispam endpoint reputation exempt
   edit <msisdn>
end
```

Variable	Description	Default
<msisdn>	Type the MSISDN number to exempt carrier end point.	

Related topics

antispam endpoint reputation blocklist

antispam greylist exempt

Use this command to configure the greylist exempt list.

Greylist scanning blocks spam based on the behavior of the sending server, rather than the content of the messages. When receiving an email from an unknown server, the FortiMail unit will temporarily reject the message. If the mail is legitimate, the originating server will try to send it again later (RFC 2821), at which time the FortiMail unit will accept it. Spam senders rarely attempt a retry.

Syntax

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

Variable	Description	Default
<entry_index>	Greylist exempt rule ID.	
recipient-pattern <recipient_pattern>	Enter a pattern that defines recipient email addresses which match this rule, surrounded in slashes and single quotes (such as `\'*\'`).	
recipient-pattern-regexp {enable | disable}	Enter `enable` if you used regular expression syntax to define the pattern. Enter `disable` if you did **not** use regular expression syntax to define the pattern (that is, you entered a complete email address, or you entered a pattern using simple wild card characters * or ?).	disable
reverse-dns-pattern <reverse-dns_pattern>	Enter a pattern that defines reverse DNS query responses which match this rule, surrounded in slashes and single quotes (such as `\'*\'`).	
reverse-dns-pattern-regexp {enable | disable}	Enter `enable` if you used regular expression syntax to define the pattern. Enter `disable` if you did **not** use regular expression syntax to define the pattern (that is, you entered a complete email address, or you entered a pattern using simple wild card characters * or ?).	disable

Variable	Description	Default
sender-ip <client_ ipv4/mask>	Enter the IP address and netmask of the SMTP client. To match SMTP sessions from any SMTP client, enter `0.0.0.0/0` (set by default).	0.0.0.0/0
sender-pattern <sender_ pattern>	Enter a pattern that defines sender email addresses which match this rule, surrounded in slashes and single quotes (such as `\'*@example.com\'`).	
sender-pattern-regexp {enable | disable}	Enter `enable` if you used regular expression syntax to define the pattern. Enter `disable` if you did **not** use regular expression syntax to define the pattern (that is, you entered a complete email address, or you entered a pattern using simple wild card characters * or ?).	disable

Related topics

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

antispam image-analysis

Use this command to configure thresholds for image scans.

When you configure a content profile, you can choose to scan images in the email body and attachments. You can fine-tune the file size that the FortiMail unit will scan, and how these images are detected. Separate thresholds exists for each category of images that you may want to block, such as violence or adult images.

Syntax

```
config antispam image-analysis
   set status {enable | disable}
   set max-size <limit_int>
   set min-size <limit_int>
   set category {alcohol drug extremism gambling gore porn swim-underwear weapon}
   set score-threshold-alcohol <score_int>
   set score-threshold-drug <score_int>
   set score-threshold-extremism <score_int>
   set score-threshold-gambling <score_int>
   set score-threshold-gore <score_int>
   set score-threshold-porn <score_int>
   set score-threshold-swimwear <score_int>
   set score-threshold-weapon <score_int>
```

```
end
```

Variable	Description	Default
category {alcohol drug extremism gambling gore porn swim-underwear weapon}	Select which categories of images to identify.	alcohol drug extremism gambling gore porn swim-underwear weapon
max-size <limit_int>	Enter the maximum image size to analyze in kilobytes (KB). Valid range is 1 to 50000. **Tip:** For a balance of fast throughput and good catch rate, use a minimum image file size that is more than small icons and email signatures, and a maximum image file size that is more than most spam and disallowed images.	500
min-size <limit_int>	Enter the minimum image size to analyze in kilobytes (KB). Valid range is 1 to 1000.	10
score-threshold <score_int>	Enter the score threshold. Valid range is 0 to 1000.	900
score-threshold-alcohol <score_int>	Enter the score threshold. Valid range is 0 to 1000.	900
score-threshold-drug <score_int>	Enter the score threshold. Valid range is 0 to 1000.	900
score-threshold-extremism <score_int>	Enter the score threshold. Valid range is 0 to 1000.	900
score-threshold-gambling <score_int>	Enter the score threshold. Valid range is 0 to 1000.	900
score-threshold-gore <score_int>	Enter the score threshold. Valid range is 0 to 1000.	900
score-threshold-porn <score_int>	Enter the score threshold. Valid range is 0 to 1000.	900
score-threshold-swimwear <score_int>	Enter the score threshold. Valid range is 0 to 1000.	900
score-threshold-weapon <score_int>	Enter the score threshold. Valid range is 0 to 1000.	900
status {enable | disable}	Enable or disable image analysis.	enable

Related topics

profile content

antispam quarantine-report

Use these commands to configure global settings for quarantine reports.

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

Alternatively, you can configure quarantine report settings specifically for each protected domain. For details, see domain-setting on page 88.

By default, insecure clear text HTTP requests to access the quarantine are redirected to secure HTTPS. See alsohttps-redirect-status {enable | disable} on page 353.

Syntax

```
config antispam quarantine-report
   set report-template-name {default | default-with-icons} on page 50
   set schedule-days {monday tuesday wednesday thursday friday saturday sunday} on page 50
   set schedule-hours {<hour_int>,...} on page 50
   set web-release-hostname <fortimail_fqdn> on page 50
   set web-release-unauth-expiry <hour_int>
end
```

Variable	Description	Default
report-template-name {default | default-with-icons}	Enter a report template.	default
schedule-days {monday tuesday wednesday thursday friday saturday sunday}	Enter a space-delimited list of days of the week on which the FortiMail unit will generate spam reports.	monday tuesday wednesday thursday friday saturday sunday
schedule-hours {<hour_int>,...}	Enter a comma-delimited list of numbers corresponding to the hours of the day on which the FortiMail unit will generate spam reports. For example, to generate spam reports on 1:00 AM, 2:00 PM, and 11:00 PM, you would enter `1,14,23`. Valid numbers are from 0 to 23, based upon a 24-hour clock.	12
web-release-hostname <fortimail_fqdn>	Enter an alternate resolvable fully qualified domain name (FQDN) to use in web release hyperlinks that appear in spam reports.	
web-release-unauth-expiry <hour_int>	Expiry time, in hours, of time limited webmail access to quarantine email without authorization. Valid values are from 0 to 720. To disable expiry, enter 0.	0

Related topics

- antispam bounce-verification
- antispam deepheader-analysis
- antispam greylist exempt
- antispam settings
- antispam trusted

antispam settings

Use these commands to configure global antispam settings.

Syntax

```
config antispam settings
   set backend-verify <time_str>
   set bayesian-is-not-spam <local-part_str>
   set bayesian-is-spam <local-part_str>
   set bayesian-learn-is-not-spam <local-part_str>
   set bayesian-learn-is-spam <local-part_str>
   set bayesian-training-group <local-part_str>
   set blocklist-action {as-profile | discard | reject}
   set bounce-verification-action {as-profile | discard | reject}
   set bounce-verification-auto-delete-policy {never | one-month | one-year | six-months | three-
       months}
   set bounce-verification-status {enable | disable}
   set bounce-verification-tagexpiry <days_int>
   set carrier-endpoint-acct-response {enable | disable}
   set carrier-endpoint-acct-secret <password_str>
   set carrier-endpoint-acct-validate {enable | disable}
   set carrier-endpoint-attribute {Acct-Authentic ... Vendor-Specific)
   set carrier-endpoint-blocklist-window-size {15m | 30m | 60m | 90m | 120m | 240m | 360m |
       480m | 1440m}
   set carrier-endpoint-framed-ip-attr {Framed-IP-Address | Login-IP-Host | Login-IPv6-Host |
       NAS-IP-Address | NAS-IPv6-Address}
   set carrier-endpoint-framed-ip-order {host-order | network-order}
   set carrier-endpoint-radius-port <port_int>
   set carrier-endpoint-status {enable | disable}
   set delete-ctrl-account <local_part_str>
   set dmarc-failure-action {use-policy-action | use-profile-action | use-profile-action-with-
       none}
   set dynamic-safe-list-domain <domain_str>
   set dynamic-safe-list-state {enable | disable}
   set greylist-capacity <maximum_int>
   set greylist-check-level {disable | enable | low | high}
   set greylist-delay <minutes_int>
   set greylist-init-expiry-period <hours_int>
   set greylist-ttl <ttl_int>
```

```
    set impersonation-analysis {manual | dynamic}
    set impersonation-analysis-level {aggressive | strict}
    set qr-code-image-max-size <kb_int>
    set qr-code-url-scan-option {attachment-image inline-image}
    set qr-code-url-scan-status {enable | disable}
    set release-ctrl-account <local-part_str>
    set safe-block-list-entry-auto-aging-status {enable | disable}
    set safe-block-list-entry-retention safe <days>
    set safe-block-list-precedence {system session domain personal}
    set safe-block-list-tracking {enable | disable}
    set safelist-bypass-sender-auth {enable | disable}
    set scan-action-preference {single-action | multi-action}
    set session-profile-rate-control-interval <minutes_int>
    set url-checking {aggressive | extreme | strict}
end
```

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

Variable	Description	Default
	For example, if the local domain name of the FortiMail unit is example.com and you want to train the Bayesian database to recognize spam by sending control messages to learn-is-spam@example.com, you would enter `learn-is-spam`.	
bayesian-training-group <local-part_str>	Enter the local-part portion of the email address that FortiMail administrators can use as their sender email address when forwarding email to the “learn is spam" email address or “learn is not spam" email address. Training messages sent from this sender email address will be used to train the global or per-domain Bayesian database (whichever is selected in the protected domain) but will **not** train any per-user Bayesian database. In contrast, if a FortiMail administrator were to forward email using their own email address (rather than the training group email address) as the sender email address, and per-user Bayesian databases were enabled in the corresponding incoming antispam profile, the FortiMail unit would also apply the training message to their own per-user Bayesian database.	default-grp
blocklist-action {as-profile | discard | reject}	Use these commands to select the action that the FortiMail unit performs when an email message arrives from or, in the case of per-session profile recipient blocklists, is destined for a blocklisted email address, mail domain, or IP address. This setting affects email matching any system-wide, per-domain, per-session profile, or per-user blocklist. For email messages involving a blocklisted email address, domain, or IP address, select one of the following options: • `as-profile`: Apply the action selected in the antispam profile being applied to the email message. For details, see profile antispam-action on page 181. • `discard`: Accept the message but delete and do not deliver it, without notifying the SMTP client. • `reject`: Reject the message, returning an SMTP error code to the SMTP client.	discard
bounce-verification-action {as-profile | discard | reject}	Enter the action that the FortiMail unit will perform if it receives a bounce address tag that is invalid. • `as-profile`: Perform the action selected in the antispam profile. • `discard`: Accept the message but then delete it without notifying the SMTP client. • `reject`: Reject the message, replying to the SMTP client with an SMTP rejection code.	as-profile

Variable	Description	Default
bounce-verification-auto-delete-policy {never | one-month | one-year | six-months | three-months}	Inactive keys will be removed after being unused for the selected time period. • `never`: Never automatically delete an unused key. • `one-month`: Delete a key when it hasn't been used for 1 month. • `three-months`: Delete a key when it hasn't been used for 3 months. • `six-months`: Delete a key when it hasn't been used for 6 months. • `one-year`: Delete a key when it hasn't been used for 12 months. The active key will not be automatically removed.	never
bounce-verification-status {enable | disable}	Enable to activate bounce address tagging and verification. Tag verification can be bypassed in IP profiles and protected domains.	disable
bounce-verification-tagexpiry <days_int>	Enter the number of days an email tag is valid. When this time elapses, the FortiMail unit will treat the tag as invalid. Valid range is from 3 to 30 days.	7
carrier-endpoint-acct-response {enable | disable}	Enable/disable endpoint account validation on the RADIUS server.	disable
carrier-endpoint-acct-secret <password_str>	Type the shared secret for RADIUS account response and request validation.	
carrier-endpoint-acct-validate {enable | disable}	Enable/disable validating shared secret of account requests.	disable
carrier-endpoint-attribute {Acct-Authentic ... Vendor-Specific)	Type the RADIUS account attribute associated with the endpoint user ID. If you have more than one RADIUS server and each server uses different account attribute for the endpoint user ID, you can specify up to five attributes with this command. For example, a 3G mobile network may use the "Calling-Station-ID" attribute while an ADSL network may use the "User-Name" attribute. A carrier end point is any device on the periphery of a carrier's or Internet service provider's (ISP) network. It could be a subscriber's GSM cellular phone, wireless PDA, or computer using DSL service.	Calling-Station-Id (RADIUS attribute 31)

Variable	Description	Default
	Unlike MTAs, computers in homes and small offices and mobile devices such as laptops and cellular phones that send email may not have a static IP address. Cellular phones' IP addresses especially may change very frequently. After a device leaves the network or changes its IP address, its dynamic IP address may be reused by another device. Because of this, a sender reputation score that is directly associated with an SMTP client's IP address may not function well. A device sending spam could start again with a clean sender reputation score simply by rejoining the network to get another IP address, and an innocent device could be accidentally blocklisted when it receives an IP address that was previously used by a spammer.	
carrier-endpoint-blocklist-window-size {15m | 30m | 60m | 90m | 120m | 240m | 360m | 480m | 1440m}	Enter the amount of previous time, in minutes, whose score-increasing events will be used to calculate the current endpoint reputation score. For example, if the window is `15m` (15 minutes), detections of spam or viruses 0-15 minutes ago would count towards the current score; detections of spam or viruses older than 15 minutes ago would not count towards the current score.	15m
carrier-endpoint-framed-ip-attr {Framed-IP-Address | Login-IP-Host | Login-IPv6-Host | NAS-IP-Address | NAS-IPv6-Address}	Specify the RADIUS attribute whose value will be used as the endpoint user IP address. By default, the endpoint user IP address uses the value of RADIUS attribute 8 (framed IP address). However, if the endpoint IP address uses the value from different RADIUS attribute name/number other than attribute 8, you can specify the corresponding attribute number with this command. You can use the command `diagnose debug application msisdn` to capture RADIUS packets and find out what attribute name/number is used to hold the IP address value. Note that you can specify multiple values, such as both IPv4 and IPv6 attributes.	Framed-IP-Address
carrier-endpoint-framed-ip-order {host-order | network-order}	Select one of the following methods for endpoint IP address formatting: • `host-order`: format an IP address in host order, that is, the host portion is at the beginning. For example, 1.1.168.192. • `network-order`: sorts IP addresses in the network order, that is, the network portion is at the begging. For example, 192.168.1.1.	host-order
carrier-endpoint-radius-port <port_int>	Type the RADIUS server port for carrier endpoint account requests.	1813
carrier-endpoint-status {enable | disable}	Enable endpoint reputation scan for traffic examined by the session profile. This command starts the endpoint reputation daemon. You must start this daemon for the endpoint reputation feature to work.	enable

Variable	Description	Default
delete-ctrl-account <local_part_str>	Use this command to configure the email addresses through which email users can delete email from their per-recipient quarantines. Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that control deletion of email from per-recipient quarantines. For example, if the local domain name of the FortiMail unit is example.com and you want to delete email by sending control messages to quar_delete@example.com, you would enter `quar_delete`.	delete-ctrl
dmarc-failure-action {use-policy-action | use-profile-action | use-profile-action-with-none}	Select either: • `use-policy-action`: Use the actions specified in policy option of the sender's DMARC record. • `use-profile-action`: Use the action specified in the antispam profile. • `use-profile-action-with-none`: If the policy option in the sender's DMARC record is `p=none`, use that action. Else use the action in the antispam profile.	use-profile-action-with-none
dynamic-safe-list-domain <domain_str>	Enter the domain name of the dynamic safe list.	
dynamic-safe-list-state {enable | disable}	Enable the dynamic safe list.	disable
greylist-capacity <maximum_int>	Enter the maximum number of greylist items in the greylist. New items that would otherwise cause the greylist database to grow larger than the capacity will instead overwrite the oldest item. To determine the default value and acceptable range for your FortiMail model, enter a question mark (?).	Varies by model
greylist-check-level {disable | enable | low | high}	Greylist scanning blocks spam based on the behavior of the sending server, rather than the content of the messages. When receiving an email from an unknown server, the FortiMail unit will temporarily reject the message. If the mail is legitimate, the originating server will try to send it again later (RFC 2821), at which time the FortiMail unit will accept it. Spammers will typically abandon further delivery attempts in order to maximize spam throughput. Enable/disable greylist check, or set how aggressively to perform greylist check: high or low. The high level setting greylists all messages from unknown MTAs, while the low level setting will selectively greylist based on the age and reputation of the MTAs: the trusted MTAs will not be greylisted whereas the new untrusted MTAs will be greylisted.	high
greylist-delay <minutes_int>	Enter the length in minutes of the greylist delay period.	10

Variable	Description	Default
	For the initial delivery attempt, if no manual greylist entry (exemption) matches the email message, the FortiMail unit creates a pending automatic greylist entry, and replies with a temporary failure code. During the greylist delay period after this initial delivery attempt, the FortiMail unit continues to reply to additional delivery attempts with a temporary failure code. After the greylist delay period elapses and before the pending entry expires (during the `initial_expiry_period`, also known as the greylist window), any additional delivery attempts will confirm the entry and convert it to an individual automatic greylist entry. The greylist scanner will then allow delivery of subsequent matching email messages. The valid range is between 1 and 120 minutes.	
greylist-init-expiry-period <hours_int>	Enter the period of time in hours after the `greylistperiod`, during which pending greylist entries will be confirmed and converted into automatic greylist entries if the SMTP client retries delivery. The valid range is between 4 to 24 hours.	4
greylist-ttl <ttl_int>	Enter the time to live (TTL) that determines the maximum amount of time that unused automatic greylist entries will be retained. Expiration dates of automatic greylist entries are determined by adding the TTL to the date and time of the previous matching delivery attempt. Each time an email message matches the entry, the life of the entry is prolonged; in this way, entries that are in active use do not expire. If the TTL elapses without an email message matching the automatic greylist entry, the entry expires and the greylist scanner removes the entry. The valid range is between 1 to 60 days.	30
impersonation-analysis {manual | dynamic}	Email impersonation is one of the email spoofing attacks. It forges the email header to deceive the recipient because the message appears to be from a different source than the actual address. To fight against email impersonation, you can map display names with email addresses and check email for the mapping. You can choose whether the impersonation analysis uses the manual mapping entries or dynamic entries. You can also use both types of entries. • `manual`: Use the entries you manually entered under *Profile > AntiSpam > Impersonation*. • `dynamic`: Use the entries automatically learned by the FortiMail mail statistics service. To enable this service, enable `mailstat-service` under `config system global`.	manual

impersonation-analysis-level {aggressive | strict}	• `aggressive`: Choose this option to check the display name email domain part in Header From.
	• `strict`: Choose this option not to check the display name email domain.
	For example, when you set an IA entry as:
	`Display name: John Smith`
	`Email address: john.smith@example.com`
		aggressive

Variable	Description	Default
	while `example.com` is a protected domain, the `aggressive` setting will block all of the following senders: • `"John Smith" <spammer@example.net>` • `"John.Smith@example.com" <spammer@example.net>` • `"OtherUser@example.com" <spammer@example.net>` but the `strict` setting will only block the first two senders.	
qr-code-image-max-size <kb_int>	Enter the maximum size (in kilobytes) to scan for QR code images that contain known spam URLs.	1000
qr-code-url-scan-option {attachment-image inline-image}	Select which location(s) to scan for QR code images that contain known spam URLs. • `inline-image`: Embedded inline, in the email body. • `attachment-image`: Email attachments.	
qr-code-url-scan-status {enable | disable}	Enable to scan for QR code images that contain known spam URLs.	disable
release-ctrl-account <local-part_str>	Use this command to configure the email addresses through which email users can release email from their per-recipient quarantines. Enter the local-part portion of the email address at which the FortiMail unit will receive email messages that control deletion of email from per-recipient quarantines. For example, if the local domain name of the FortiMail unit is example.com and you want to delete email by sending control messages to quar_delete@example.com, you would enter `quar_delete`.	
safe-block-list-entry-auto-aging-status {enable | disable}	Enable to apply automatic purging of system and domain block and safe lists that are listed for a defined retention period (see safe-block-list-entry-retention safe <days>).	enable
safe-block-list-entry-retention safe <days>	Enter the retention period in days for safe and block list entries before they are automatically removed. Set the value between 1-365.	120
safe-block-list-precedence {system session domain personal}	By default, system safelists and blocklists have precedence over other safelists and blocklists. In some cases, you may want to change the precedence order. For example, you may want to allow a user to use their own lists to overwrite the system list. In this case, you can move “personal’ ahead of “system”.	system session domain personal
safe-block-list-tracking {enable | disable}	Enable to track various system safelist and blocklist statistics, including creation time, last hit time, and hit count. These statistics are tracked on *Security >Block/Safe List > System* and *Security > Block/Safe List > Domain*.	disable

Variable	Description	Default
safelist-bypass-sender-auth {enable | disable}	Enable to bypass sender authentication mechanism (SPF/DMARC/DKIM) for safelisted senders. When disabled, if the scan result of SPF, DKIM, or DMARC is a failure, and the sender is safelisted, the result of SPF, DKIM, and DMARC takes precedence.	enable
scan-action-preference {single-action | multi-action}	Either apply only the first matching antispam filter, or multiple matching antispam filters, where each matching antispam filter action is applied until the final action is found.	multi-action
session-profile-rate-control-interval <minutes_int>	The rate control option enables you to control the rate at which email messages can be sent, by the number of connections, the number of messages, or the number recipients per client per period (in minutes). This command sets the time period. Other settings are in `config profile session`.	30
url-checking {aggressive | extreme | strict}	If you enable a FortiGuard scan or SURBL scan in an antispam profile, then FortiMail scans for blocklisted URLs in the email message body. Types of URLs that URL filtering can scan include: • **Absolute URLs** — URL syntax with scheme name (protocol), such as `http`, `https`, and `ftp`. They often only include a domain name. Example: `http://www.example.com` • **Reference URLs** — No scheme name. Example: `example.com` URLs in email can also be written in plain text instead of as clickable HTML links. While not technically a URL, the domain name of the sender can also be inspected. By default, FortiMail scans for absolute URLs only. If you need to improve the spam catch rate or reduce false positives, you can change this. Select which to scan for. • `strict`: Absolute URLs only. **Note:** Websites without “http” or “https” but starting with “www” are also treated as absolute URLs. Example: `www.example.com` • `aggressive`: Like `strict`, but also inspect reference URLs. Also check the domain name of the sender in the SMTP envelope (`MAIL FROM:`) and message header (`From:` and `Reply-To:`). • `extreme`: Like `aggressive`, but also inspect URLs in plain text format.	strict

Related topics

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

antispam trusted

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

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

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

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

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

Syntax

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

Variable	Description	Default
<smtp_ipv4/mask>	Enter the IP address and netmask of an MTA.	

Related topics

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

antispam url-fgas-exempt-list

Use this command to create a list of URLs that are exempt from FortiGuard Antispam rating.

Syntax

```
config antispam url-fgas-exempt-list
   edit <list_id>
      set pattern-type
      set url-exempt-pattern
end
```

Variable	Description	Default
<list_id>	Enter the identifier for the entry in the list.	
pattern-type	Enter the pattern type.	
url-exempt-pattern	Enter either a URL or a pattern that matches URLs that will be exempt from FortiGuard Antispam rating.	

Related topics

archive exempt-policy

archive policy

profile antispam-action

profile content-action

archive account

Use this command to configure email archiving accounts.

This command applies only if email archiving is enabled.

Syntax

```
config archive account
   edit <account_name>
      set destination {local | remote}
      set forward-address <recipient_email>
      set imap-access {enable | disable}
      set index-type {full | header |none}
      set local-quota <quota_int>
      set local-quota-cache <cache_int>
      set password <password_str>
      set quota-full {overwrite | noarchive}
      set remote-directory <path_str>
      set remote-ip <ftp_ipv4>
      set remote-password <password_Str>
      set remote-protocol {ftp |  sftp}
```

```
        set remote-username <user_str>
        set retention-period <time_int>
        set rotation-hour <hour_int>
        set rotation-size <size_int>
        set rotation-time <time_int>
        set status {enable | disable}
end
```

Variable	Description	Default
<account_name>	Enter the email archiving account name.	archive
destination {local | remote}	Select whether to archive to the local disk or remote server.	local
forward-address <recipient_email>	Enter the email address to which all archived messages will also be forwarded. If no forwarding address exists, the FortiMail unit will not forward email when it archives it.	
imap-access {enable | disable}	Enable/disable IMAP access to the archive account.	disable
index-type {full | header |none}	Type `full` to index email by the whole email (header and body), and `header` by the email header only.	none
local-quota <quota_int>	Enter the local disk quota for email archiving in gigabytes (GB). The valid range depends on the amount of free disk space.	5
local-quota-cache <cache_int>	Enter the local disk quota for caching in gigabytes (GB). The valid range depends on the amount of free disk space.	5
password <password_str>	Enter the archiving account's password.	forti12356net
quota-full {overwrite | noarchive}	Enter either: `noarchive`: Discard the email message if the hard disk space is consumed and a new email message arrives. `overwrite`: Replace the oldest email message if the hard disk space is consumed and a new email message arrives.	overwrite
remote-directory <path_str>	Enter the directory path on the remote server where email archives will be stored.	
remote-ip <ftp_ipv4>	Enter the IP address of the remote server that will store email archives.	0.0.0.0
remote-password <password_Str>	Enter the password of the user account on the remote server.	

Variable	Description	Default
remote-protocol {ftp | sftp}	Enter either `ftp` or `sftp` to use that protocol when transferring email archives to the remote server.	sftp
remote-username <user_str>	Enter the name of a user account on the remote server.	
retention-period <time_int>	Enter the maximum age in days that rotated archive folders are kept before they are removed. The valid range is from 0 to 3650 days. The default value of `0` means no archive folders will be removed.	365
rotation-hour <hour_int>	Enter the hour of the day to start the mailbox rotation. See rotation-time <time_int>.	0
rotation-size <size_int>	Enter the maximum size of the current email archiving mailbox in megabytes (MB). When the email archiving mailbox reaches either the maximum size or age, the email archiving mailbox is rolled (that is, the current email archiving mailbox is saved to a file with a new name, and a new email archiving mailbox is started). The valid range is from 10 to 800 MB.	200
rotation-time <time_int>	Enter the maximum age of the current email archiving mailbox in days. When the email archiving mailbox reaches either the maximum size or age, the email archiving mailbox is rolled (that is, the current email archiving mailbox is saved to a file with a new name, and a new email archiving mailbox is started). The valid range is from 1 to 365 days. See rotation-hour <hour_int>	7
status {enable | disable}	Enable to activate email archiving.	enable

Related topics

archive exempt-policy
archive journal

archive exempt-policy

Use this command to configure the exemptions to email archiving.

This command applies only if email archiving is enabled.

Syntax

```
config archive exempt-policy
   edit <policy_id>
      set account <account_name>
      set pattern <pattern_Str>
      set status {enable | disable}
      set type {sender | recipient | spam}
end
```

Variable	Description	Default
<policy_id>	Enter the index number of the exemption policy. To view a list of existing entries, enter a question mark (?).	
account <account_name>	Enter the name of the email archive account that you want to apply the exemption policy to.	
pattern <pattern_Str>	Enter a pattern, such as `user*@example.com`, that matches the attachment file name, text in the email body, text in the email subject, sender or recipient email addresses to which this exemption will apply.	*
status {enable | disable}	Enable to activate the email archiving exemption.	enable
type {sender | recipient | spam}	Enter the match type, either: • `sender`: The sender email address will be evaluated for matches with `pattern`. • `recipient`: The recipient email address will be evaluated for matches with `pattern`. • `spam`: Do not archive spam emails.	sender

Related topics

archive journal

antispam url-fgas-exempt-list

archive journal

Microsoft Exchange servers can journal email and then send the journaled email to another server, such as FortiMail, for archiving.

Syntax

```
config archive journal source
```

```
    edit <journal_source_id>
       set comments
       set email-archive-status {enable | disable}
       set email-continuity-status {enable | disable}
       set host
       set recipient
       set scan-status {enable | disable}
       set sender
       set status {enable | disable}
end
```

Variable	Description	Default
<journal_source_id>	Enter the ID of the journal.	
comments	Enter general journal source comments.	
email-archive-status {enable | disable}	Enable or disable email archival of journal reports.	enable
email-continuity-status {enable | disable}	Enable or disable email continuity, taking email from journal reports to users' mailboxes. When enabled, users can access inbound emails in instances where the email server protected by the FortiMail unit goes offline. **Note:** This command is only available when the FortiMail unit is operating in either gateway or transparent mode.	disable
host	Enter the ip address or host name of the journal source.	
recipient	Enter the recipient email address.	
scan-status {enable | disable}	Enable or disable scanning of embedded emails within journal reports.	disable
sender	Enter the sender email address.	
status {enable | disable}	Enable or disable the journal source.	enable

archive policy

Use this command to configure email archiving policies.

This command applies only if email archiving is enabled.

Syntax

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

```
        set deferral-reason {spam-outbreak virus-outbreak sandbox}
end
```

Variable	Description	Default
<policy_id>	Enter the index number of the policy. To view a list of existing entries, enter a question mark (?).	
account <account_name>	Enter the name of the email archive account where you want to archive email.	
pattern <string>	Enter a pattern, such as `user*@example.com`, that matches the attachment file name, text in the email body, text in the email subject, sender or recipient email addresses to which this policy will apply.	*
status {enable | disable}	Enable to activate the email archiving policy.	enable
type {attachment | body | deferral | recipient | sender | subject}	Select either: • `attachment`: The attachment file name will be evaluated for matches with `pattern`. • `body`: The body text will be evaluated for matches with `pattern`. • `deferral`: The archive policy will be evaluated for matches with `deferral-reason`. • `recipient`: The recipient email address will be evaluated for matches with `pattern`. • `sender`: The sender email address will be evaluated for matches with `pattern`. • `subject`: The email subject will be evaluated for matches with `pattern`.	sender
deferral-reason {spam-outbreak virus-outbreak sandbox}	Note that this option is only available when `type` is set to `deferral`. Enter one or more of the following reasons for deferring emails for analysis: • `fortisandbox`: Defer email for sandbox scanning. • `spam-outbreak`: Defer email for spam outbreak. • `virus-outbreak`: Defer email for virus outbreak.	

Related topics

archive exempt-policy

antispam url-fgas-exempt-list

calendar server

Use this command to enable WebDAV and CalDAV support, allowing the ability to share calendars.

Syntax

```
config calendar server
   set webdav-status {enable | disable}
   set caldav-status {enable | disable}
end
```

Variable	Description	Default
webdav-status {enable | disable}	Enable or disable WebDAV support.	enable
caldav-status {enable | disable}	Enable or disable CalDAV support.	enable

cloud-api account

Use this command to connect to Microsoft 365 and Google Workspace to access the user mailboxes.

You must have domain administrator privileges to access Microsoft 365 or Google Workspace.

Syntax

```
config cloud-api account
   edit <profile_name>
      [set description <comment_str>
      set status {enable | disable}
      set type {exchange | ms365 | gmail}
      set admin-email <administrator_email>
      set application-id <id_str>
      set application-key <key_str>
      set application-secret <password_str>
      set tenant <password_str>
      set global-address-list <id_str>
      set realtime-scan-status {enable | disable}
      set service-email <service_email>
      set service-endpoint {china | germany | global | us-dod | us-gov}
      set service-password <password_str>
      set service-url <service_url>
      config user-filter
         edit <user-filter_name>
            set status {enable | disable}
            set type {ad-group | email-group | imported-user | ldap-group | regex | wildcard}
            set ad-group-attr {custom | displayname | mail}
            set ad-group-attr-name <attribute-name_str>
            set ad-group-attr-value <attribute-value_str>
            set email-group <group_name>
            set ldap-group <group_str>
            set ldap-profile <profile_name>
            set pattern <user-filter_pattern>
         next
      end
```

```
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile.	
admin-email <administrator_email>	Enter the email address of the administrator. This setting is only available if type {exchange | ms365 | gmail} is `gmail`.	
application-id <id_str>	Enter the application ID. This setting is only available if type {exchange | ms365 | gmail} is `ms365`.	
application-key <key_str>	This setting is only available if type {exchange | ms365 | gmail} is `gmail`.	
application-secret <password_str>	Enter the application secret or password. This setting is only available if type {exchange | ms365 | gmail} is `ms365`.	
description <comment_str>	Enter a description of the account.	
email-group <group_name>	Enter an email group name. This setting is only available if type {ad-group | email-group | imported-user | ldap-group | regex | wildcard} is `email-group`.	
global-address-list <id_str>	Enter the ID of a global address list. This setting is only available if type {exchange | ms365 | gmail} is `exchange`.	
ldap-group <group_str>	Enter the LDAP group name. This setting is only available if type {ad-group | email-group | imported-user | ldap-group | regex | wildcard} is `ldap-group`.	
ldap-profile <profile_name>	Select an LDAP group profile. This setting is only available if type {ad-group | email-group | imported-user | ldap-group | regex | wildcard} is `ldap-group`.	
realtime-scan-status {enable | disable}	Enable or disable real-time scan.	enable
service-email <service_email>	Enter the email address used to log into the service. This setting is only available if type {exchange | ms365 | gmail} is `exchange`.	
service-endpoint {china | germany | global | us-dod | us-gov}	Select a regional endpoint for your geographical location and regulatory compliance requirements. This setting is only available if type {exchange | ms365 | gmail} is `ms365`.	global
service-password <password_str>	Enter the password used to log into the service.	

Variable	Description	Default
	This setting is only available if type {exchange | ms365 | gmail} is exchange.	
service-url <service_url>	Enter the URL used to log into the service. This setting is only available if type {exchange | ms365 | gmail} is exchange.	
status {enable | disable}	Enable or disable this account.	enable
tenant <password_str>	Enter the Microsoft 365 tenant credentials.	
type {exchange | ms365 | gmail}	Select whether the account is on Microsoft 365, Microsoft Exchange, or Google Workspace.	ms365
<user-filter_name>	Enter the name of the user filter.	
pattern <user-filter_pattern>	Enter the user filter pattern. This setting is only available if type {ad-group | email-group | imported-user | ldap-group | regex | wildcard} is regex or wildcard.	
ad-group-attr {custom | displayname | mail}	Select the Microsoft Azure Entra ID (formerly Active Directory) group attribute. This setting is only available if type {ad-group | email-group | imported-user | ldap-group | regex | wildcard} is ad-group.	displayname
ad-group-attr-name <attribute-name_str>	Enter the custom Microsoft Azure Entra ID (formerly Active Directory) group attribute name. This setting is only available when both: • type {ad-group | email-group | imported-user | ldap-group | regex | wildcard} is ad-group • ad-group-attr {custom | displayname | mail} is custom	
ad-group-attr-value <attribute-value_str>	Enter the Microsoft Azure Entra ID (formerly Active Directory) group attribute value. This setting is only available if type {ad-group | email-group | imported-user | ldap-group | regex | wildcard} is ad-group.	
status {enable | disable}	Enable or disable this user filter.	disable
type {ad-group | email-group | imported-user | ldap-group | regex | wildcard}	Select the user filter type, either: • ad-group: Microsoft Azure Entra ID (formerly Active Directory) group. • email-group: Email group. • imported-user: Imported internal or external user. • ldap-group: LDAP group. • regex: Regular expression. • wildcard:Wildcard.	wildcard

cloud-api policy

Use this command to configure Microsoft 365 and Google Workspace scan policies. You must have domain administrator privileges to access Microsoft 365 or Google Workspace.

Syntax

```
config cloud-api policy
   edit <policy_index>
      set status {enable | disable}
      [set comment "<comment_str>"]
      set account <account_name>
      set source-type {geoip-group | ip-address | ip-group}
      set source-ip-address {<client_ipv4mask> | <client_ipv6mask>}
      set source-ip-group <ip-group_name>
      set source-geoip-group <geoip-group_name>
      set sender-type {ad-group | email-group | external | internal | ldap-group | regex |
          wildcard}
      set sender-name <username_str>
      set sender-domain <sender_fqdn>
      set sender-ad-group-attr {custom | displayname | mail}
      set sender-ad-group-attr-name <attribute-name_str>
      set sender-ad-group-attr-value <attribute-value_str>
      set sender-email-group <group_name>
      set sender-ldap-profile <profile_name>
      set sender-pattern-regex <sender_pattern>
      set recipient-type {ad-group | email-group | ldap-group | regex | wildcard}
      set recipient-name <username_str>
      set recipient-domain <recipient_fqdn>
      set recipient-ad-group-attr {custom | displayname | mail}
      set recipient-ad-group-attr-name <attribute-name_str>
      set recipient-ad-group-attr-value <attribute-value_str>
      set recipient-email-group <group_name>
      set recipient-ldap-profile <profile_name>
      set recipient-pattern-regex <recipient_pattern>
      set profile-antispam <profile_name>
      set profile-antivirus <profile_name>
      set profile-content <profile_name>
      set profile-dlp <profile_name>
end
```

Variable	Description	Default
<policy_index>	Enter an index number for the policy in the table.	
account <account_name>	Select the name of a Microsoft 365 or Google Workspace account.	
comment "<comment_str>"	Enter a description or comment.	
profile-antispam <profile_	Select which antispam profile this policy will apply.	

Variable	Description	Default
name>		
profile-antivirus <profile_name>	Select which antivirus profile this policy will apply.	
profile-content <profile_name>	Select which content profile this policy will apply.	
profile-dlp <profile_name>	Select which DLP profile this policy will apply.	
recipient-ad-group-attr {custom | displayname | mail}	Select which attribute contains email addresses in your Microsoft Azure Entra ID (formerly Active Directory) directory schema, either: • `displayname` • `mail` • `custom` — A custom attribute. Also configure recipient-ad-group-attr-name <attribute-name_str>. **Note:** This setting is only available when recipient-type {ad-group | email-group | ldap-group | regex | wildcard} is `ad-group`.	displayname
recipient-ad-group-attr-name <attribute-name_str>	Enter the name of the custom attribute. **Note:** This setting is only available when recipient-type {ad-group | email-group | ldap-group | regex | wildcard} is `ad-group` and recipient-ad-group-attr {custom | displayname | mail} is `custom`.	
recipient-ad-group-attr-value <attribute-value_str>	Enter the attribute value that will match this policy. **Note:** This setting is only available when recipient-type {ad-group | email-group | ldap-group | regex | wildcard} is `ad-group`.	
recipient-domain <recipient_fqdn>	Enter the domain part of the recipient email address.	*
recipient-email-group <group_name>	Select an email address group. **Note:** This setting is only available when recipient-type {ad-group | email-group | ldap-group | regex | wildcard} is `email-group`.	
recipient-ldap-profile <profile_name>	Select an LDAP profile. **Note:** This setting is only available when recipient-type {ad-group | email-group | ldap-group | regex | wildcard} is `ldap-group`.	
recipient-name <username_str>	Depending on how you chose to define matching email addresses, enter either the: • Local part (username) of the email address, or a wild card pattern. Wild card patterns allow you to match multiple email addresses. An asterisk (*) matches one or more characters; a question mark (?) matches any one character. • Group's full or partial membership attribute value, as it	*

Variable	Description	Default
	appears in your LDAP directory. Depending on the schema and group-relative-name {enable | disable}, the format is either: • `admins` • `cn=admins,ou=Groups,dc=example,dc=com` **Note:** This setting is only available when recipient-type {ad-group | email-group | ldap-group | regex | wildcard} is `wildcard` or `ldap-group`.	
recipient-pattern-regex <recipient_pattern>	Enter a regular expression that matches only email addresses that this policy should apply to. See also regular expression syntax and examples in the FortiMail Administration Guide. **Tip:** To test and validate the regular expression, you can use the FortiMail GUI. **Note:** This setting is only available when recipient-type {ad-group | email-group | ldap-group | regex | wildcard} is regex.	
recipient-type {ad-group | email-group | ldap-group | regex | wildcard}	Select how you want to define the recipient email addresses that match this policy, either: • `ad-group` — Group in a Microsoft Azure Entra ID (formerly Active Directory) directory. Also configure recipient-ad-group-attr {custom | displayname | mail} and recipient-ad-group-attr-value <attribute-value_str>. • `email-group` — Email address group configured on FortiMail.Also configure recipient-email-group <group_name>. • `ldap-group` — Group in an LDAP directory. Also configure recipient-name <username_str> and recipient-ldap-profile <profile_name>. • `regex` — Regular expression. Also configure recipient-pattern-regex <recipient_pattern>. • `wildcard` — Email address or a wild card pattern. Also configure recipient-name <username_str> and recipient-domain <recipient_fqdn>.	wildcard
sender-ad-group-attr {custom | displayname | mail}	Select which attribute contains email addresses in your Microsoft Azure Entra ID (formerly Active Directory) directory schema, either: • `displayname` • `mail` • `custom` — A custom attribute. Also configure sender-ad-group-attr-name <attribute-name_str> **Note:** This setting is only available when sender-type {ad-group | email-group | external | internal | ldap-group | regex | wildcard} is `ad-group`.	displayname

Variable	Description	Default
sender-ad-group-attr-name <attribute-name_str>	Enter the name of the custom attribute. **Note:** This setting is only available when sender-type {ad-group | email-group | external | internal | ldap-group | regex | wildcard} is `ad-group` and sender-ad-group-attr {custom | displayname | mail} is `custom`.	
sender-ad-group-attr-value <attribute-value_str>	Enter the attribute value that will match this policy. **Note:** This setting is only available when sender-type {ad-group | email-group | external | internal | ldap-group | regex | wildcard} is `ad-group`.	
sender-domain <sender_fqdn>	Enter the domain part of the sender email address.	*
sender-email-group <group_name>	Select an email group. **Note:** This setting is only available when sender-type {ad-group | email-group | external | internal | ldap-group | regex | wildcard} is `email-group`.	
sender-ldap-profile <profile_name>	Select an LDAP profile. **Note:** This setting is only available when sender-type {ad-group | email-group | external | internal | ldap-group | regex | wildcard} is `ldap-group`.	
sender-name <username_str>	Depending on how you chose to define matching email addresses, enter either the: • Local part (username) of the email address, or a wild card pattern. Wild card patterns allow you to match multiple email addresses. An asterisk (*) matches one or more characters; a question mark (?) matches any one character. • Group's full or partial membership attribute value, as it appears in your LDAP directory. Depending on the schema and group-relative-name {enable | disable}, the format is either: • `admins` • `cn=admins,ou=Groups,dc=example,dc=com` **Note:** This setting is only available when sender-type {ad-group | email-group | external | internal | ldap-group | regex | wildcard} is `wildcard` or `ldap-group`.	*
sender-pattern-regex <sender_pattern>	Enter a regular expression that matches only email addresses that this policy should apply to. See also regular expression syntax and examples in the FortiMail Administration Guide. **Tip:** To test and validate the regular expression, you can use the FortiMail GUI.	

Variable	Description	Default
	Note: This setting is only available when sender-type {ad-group | email-group | external | internal | ldap-group | regex | wildcard} is `regex`.	
sender-type {ad-group | email-group | external | internal | ldap-group | regex | wildcard}	Select how you want to define the sender email addresses that match this policy, either: • `ad-group` — Group in a Microsoft Azure Entra ID (formerly Active Directory) directory. Also configure recipient-ad-group-attr {custom | displayname | mail} and recipient-ad-group-attr-value <attribute-value_str>. • `email-group` — Email address group configured on FortiMail.Also configure recipient-email-group <group_name>. • `external` — Email address that does not belong to the protected domain. • `internal` — Email addressthat belongs to the protected domain. • `ldap-group`: Group in an LDAP directory. Also configure recipient-name <username_str> and recipient-ldap-profile <profile_name>. • `regex`:Regular expression. Also configure recipient-pattern-regex <recipient_pattern>. • `wildcard`: Email address or a wild card pattern. Also configure recipient-name <username_str> and recipient-domain <recipient_fqdn>.	wildcard
source-ip-address {<client_ipv4mask> | <client_ipv6mask>}	Enter the SMTP client IP address and netmask. To match all clients, enter `0.0.0.0/0`. **Note:** This setting is only available when source-type {geoip-group | ip-address | ip-group} is `ip-address`.	0.0.0.0/0
source-ip-group <ip-group_name>	Select which IP address group to use. **Note:** This setting is only available when source-type {geoip-group | ip-address | ip-group} is `ip-group`.	
source-geoip-group <geoip-group_name>	Select which GeoIP group to use. **Note:** This setting is only available when source-type {geoip-group | ip-address | ip-group} is `geoip-group`.	
source-type {geoip-group | ip-address | ip-group}	Select how you want to define the source IP addresses of SMTP clients that will match this policy, either: • IP address and netmask • IP address group • GeoIP group	ip-address
status {enable | disable}	Enable or disable the policy.	disable

Related topics

- domain
- profile antispam
- profile antivirus
- profile content
- profile dlp
- profile geoip-group
- profile ip-address-group
- profile ldap
- policy recipient

cloud-api profile action

Use this command to apply specific actions the unit takes when encountering an infected email. The actions applied on Microsoft 365 and Google Workspace are different from those applied on the FortiMail unit itself.

Syntax

```
config cloud-api profile action
   edit <profile_name>
      set final-action {discard | move | none | personal-quarantine | system-quarantine}
      set move-to-folder-name <path_str>
      set notification-profile <profile_name>
      set notification-status {enable | disable}
      set replace-message <replacement-message_name>
      set replace-status {enable | disable}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the action profile or create a new one.	
final-action {discard | move | none | personal-quarantine | system-quarantine}	Enter one of the following final actions to perform on infected emails: • `discard`: Move the email message from the user's inbox to the Junk folder on Microsoft 365 or Google Workspace. • `move`: Move the email message from the user's inbox to a specified folder on Microsoft 365 or Google Workspace. See move-to-folder-name <path_str>. • none: No action is taken. • `personal-quarantine`: Create a bulk folder for the user on Microsoft 365 or Google Workspace and move the email message from the user's inbox to their Bulk folder.	

Variable	Description	Default
	• `system-quarantine`: Send a copy to the FortiMail system quarantine folder and move the email message from the user's inbox to the Deleted items folder in Microsoft 365 or Google Workspace.	
move-to-folder-name <path_str>	Enter the name of the folder that the email messages should be moved to. Only applicable when `final-action` is set to `move`.	
notification-profile <profile_name>	Enter to send out notifications to the recipients specified in the notification profile.	
notification-status {enable | disable}	Enable or disable the notification.	disable
replace-message <replacement-message_name>	Enter the name of the custom message for content replacement.	default
replace-status {enable | disable}	Enable or disable the content replacement.	disable

cloud-api profile antispam

Use this command to configure the antispam profile for the administrator account of the Microsoft 365 and Google Workspace domain.

See profile antispam for more details on commands and descriptions.

cloud-api profile antivirus

Use this command to create antivirus profiles that you can select in a policy in order to scan email for viruses for the administrator account of the Microsoft 365 and Google Workspace domain.

See profile antivirus for more details on commands and descriptions.

cloud-api profile weighted-analysis

Use this command to configure weighted analysis profiles for the administrator account of the Microsoft 365 and Google Workspace domain. To avoid false positives and false negatives, you can adjust the scores ("weight") of each type of suspicious behavior, and the total score threshold that an email must reach to be categorized as spam.

To use a weighted analysis profile, select it in an antispam profile.

Syntax

```
config profile weighted-analysis
   edit <profile_name>
      set comment <comment_str>
      config rule
         edit <order_index>
            set name <rule_name>
            set status {enable | disable}
            set action <profile_name>
            set threshold <score_float>
            set action-keyword-score <score_float>
            set cousin-domain-score <score_float>
            set dictionary-profile <profile_name>
            set dictionary-threshold <score_int>
            set intelligent-analysis-score <score_float>
            set malformed-email-score <score_float>
            set sender-alignment-score <score_float>
            set suspicious-character-score <score_float>
            set url-profile <profile_name>
            set url-profile-score <score_float>
         next
      end
   next
end
```

Syntax

Variable	Description	Default
<profile_name>	Enter the name of the weighted-analysis profile.	
comment <comment_str>	Enter a descriptive comment.	
<order_index>	Enter the numerical order of the rule in the profile.	
name <rule_name>	Enter a name for the rule.	
status {enable | disable}	Enable or disable the rule.	enable
action <profile_name>	Enter the name of an action profile.	

Variable	Description	Default
threshold <score_float>	Enter the minimum total score that triggers the action. The total score is determined by adding the scores of all categories (suspicious character, etc.) in the weighted analysis rule.	50.000000
action-keyword-score <score_float>	Enter a weight-adjusted score for dictionary profile matches.	10.000000
cousin-domain-score <score_float>	Enter a weight-adjusted score for domain name impersonation. See also profile cousin-domain on page 211.	10.000000
dictionary-profile <profile_name>	Enter the name of a dictionary profile. The dictionary profile contains keywords (for example, "Click here", "Transfer", "Money", "Dollars", "Bank account", etc.) that ask the user to perform an action that typically only spammers ask for, and therefore are suspicious.	
dictionary-threshold <score_int>	Enter a weight-adjusted score for dictionary profile matches.	1
intelligent-analysis-score <score_float>	Enter a weight-adjusted score for intelligent analysis detections. Multiple factors contribute to and inform the intelligent analysis condition, in order to detect fewer false positive results, including SPF, DKIM, DMARC, alignment of sender addresses in the message header (`From:` and `Reply-To:`), new web filter domains, header analysis, and malformed emails.	50.000000
malformed-email-score <score_float>	Enter a weight-adjusted score for malformed emails. Malformed emails are those emails that contain malformed data in the email structure, header, or body. For more information, see RFC 7103.	10.000000
sender-alignment-score <score_float>	Enter a weight-adjusted score for sender domain mismatches. Sender alignment compares the domain name of the sender email address in the message header (`From:`) and SMTP envelope (`MAIL FROM:`) to look for a mismatch, which is typical of spam.	10.000000
suspicious-character-score <score_float>	Enter a weight-adjusted score for suspicious characters. Protects against internationalized domain name (IDN) homograph attacks. If domain names in URLs, sender email addresses, or recipient email addresses have Unicode characters that are from different languages yet look similar (for example, `A` looks similar in Cyrillic, Greek, and Latin alphabets), then an attacker could trick the user into using a fraudulent website or email. FortiMail detects these as suspicious.	10.000000

Variable	Description	Default
url-profile <profile_name>	Enter the name of a URL category profile.	unrated
url-profile-score <score_float>	Enter a weight-adjusted score for URL category profile matches.	10.000000

cloud-api profile content

Use this command to create content profiles, which you can use to match email based upon its subject line, message body, and attachments.

See profile content for details on commands and descriptions.

cloud-api profile dlp

Use this command after you configure the scan rules/conditions. Add the scan rules/conditions to the DLP profiles. In the profiles, you also specify what actions to take. Then you apply the DLP profiles to the IP or recipient based policies.

See profile dlp for more details on commands and descriptions.

cloud-api setting

Use this command to configure real-time scan settings.

Syntax

```
config cloud-api setting
   set hide-email-on-arrival {enable | disable}
   set push-notification-url-base <url_str>
   set realtime-scan-log {all | on-policy-match}
   set realtime-scan-status {enable | disable}
   set service-endpoint {china | germany | global | us-dod | us-gov}
   set system-quarantine-release-original {enable | disable}
end
```

Variable	Description	Default
hide-email-on-arrival {enable | disable}	Enable or disable moving email to hidden folder on arrival for real-time scan. When enabled, this feature helps to avoid users opening potentially dangerous email before the FortiMail unit has had the opportunity to scan the email, especially if the email contains large attachments. After the email is scanned and deemed safe, it is then removed from the hidden folder and placed into the user's mailbox. **Note**: This option is only available for Microsoft 365.	disable
push-notification-url-base <url_str>	Define the base URL to receive notifications.	
realtime-scan-log {all | on-policy-match}	Enter a real-time scan log option. When set to `on-policy-match`, Microsoft 365 and Google Workspace History, Mail Event, Antivirus, and Antispam log entries will only be logged upon policy match.	on-policy-match
realtime-scan-status {enable | disable}	Enable or disable real-time scans.	disable
service-endpoint {china | germany | global | us-dod | us-gov}	Enter the appropriate geographical Microsoft 365 or Google Workspace service endpoint.	global
system-quarantine-release-original {enable | disable}	Enable to release quarantined email in its original format from Microsoft 365 to the end user. If disabled, or if the email is released to other recipients, Microsoft 365 emails are released as notification emails with the original email attached as an EML file. All the tenant, user, and message GUIDs are stored in the FortiMail system quarantine. **Note**: This option is only available for Microsoft 365.	enable

customized-message

Use this command to customize text on the FortiMail unit and the email that it processes.

Custom messages are used in many places such as login pages, IBE messages, disclaimer messages, email templates, and other system-related messages.

There is a limit of 8191 characters for each custom message.

Syntax

```
config customized-message
   edit <customized-message-type_name>
      config variable
         edit %%<variable_name>%%
            set display-name "<gui-label_str>"
            set content "<text_str>"
         next
      end
      config {email-template | message}
         edit {<email-template_name> | <message_name>}
            [set description "<comment_str>"]
            set env-from <sender_email>
            set env-to <recipient_email>
            set from <sender_email>
            set to <recipient_email>
            set subject "<text_str>"
            set subject-tag-status {enable | disable}
            set subject-tag "<text_str>"
            set header-insertion-status {enable | disable}
            set header-name <key_str>
            set header-value "<text_str>"
            set status {enable | disable}
            set location {beginning | end}
            set format {html | multiline | text}
            set content "<text_str>"
            set html-body "<text_str>"
            set text-body "<text_str>"
         next
      end
   next
end
```

Variable	Description	Default
<customized-message-type_name>	Enter the name of a message that you want to customize, such as `alert-email` or `disclaimer-insertion`. Many predefined message types exist. To display the full list of options, enter: `edit ?`	
%%<variable_name>%%	Enter the variable name to use in the custom message. For example, if you enter `%%COMPANY-NAME%%`, also use that same text in the custom message if you insert it. This is also the name of the variable as it appears in the CLI. (The GUI uses display-name "<gui-label_str>" instead.) Many predefined variables exist, and you cannot edit their values or rename them. Variables cannot be reused in other messages or email templates. For a list of predefined variables and which templates they can be used in, see the FortiMail Administration Guide.	
{email-template | message}	Select a type that matches what you entered in <customized-message-type_name>, either: • `message` — Text labels used in the administrator or webmail user GUI, or	

Variable	Description	Default
	inside an email to explain when content or attachments were blocked. • `email-template` — An email template. Settings inside this sub-command vary by this selection.	
{<email-template_name> | <message_name>}	Enter the name of the email template or message. Valid inputs are usually only existing names; you cannot create a new entry. Exceptions include types where new messages can be configured and selected. For example, if <customized-message-type_name> is `disclaimer-insertion`, then you may want to configure multiple disclaimer messages, both system-wide and for specific protected domains.	
content "<text_str>"	Enter the value of the variable or custom message.	
description "<comment_str>"	Enter a comment or description. This setting is available only if {<email-template_name> | <message_name>} is `disclaimer-insertion`.	
display-name "<gui-label_str>"	Enter a label that will appear in the variable list when you click *Insert Variables* in the GUI while customizing a message or creating a variable. For example, you could enter `Company Name` for the variable `%%COMPANY-NAME%%`.	
env-from <sender_email>	Enter the sender email address (`MAIL FROM:`) that will be used in the SMTP envelope. You can either enter text directly, or insert a variable such as `%%ORIG_ENVELOPE_FROM%%`. This setting is available only for email templates.	
env-to <recipient_email>	Enter the recipient email address (`MAIL TO:`) that wil be used in the SMTP envelope. You can either enter text directly, or insert a variable such as `%%ORIG_ENVELOPE_TO%%`. This setting is available only for email templates.	
format {html | multiline | text}	Select the format of the email. This setting is available only for email templates.	html
from <sender_email>	Enter the sender email address (`From:`) that will be used in the message header. You can either enter text directly, or insert a variable such as `%%POSTMASTER%%`. Can be up to 60 characters. This setting is available only for email templates.	
header-insertion-status {enable | disable}	Enable or disable insertion of a header line. Also configure header-name <key_str> and header-value "<text_str>". This setting is available only if {<email-template_name> | <message_name>} is `disclaimer-insertion`.	disable
header-name <key_str>	Enter the key of the header line. For example, in this header: `X-Corp-News: Daily` the key is `X-Corp-News`.	
header-value "<text_str>"	Enter the value of the header. For example, in this header: `X-Corp-News: Daily`	

Variable	Description	Default
	the value is `Daily`.	
html-body "<text_str>"	Enter the body that will be used in the HTML format version of the email. Can be up to 4000 characters. This setting is available only for email templates.	
location {beginning | end}	Select where in the message body to insert the custom message. This setting is available only if {<email-template_name> | <message_name>} is `disclaimer-insertion`.	beginning
subject "<text_str>"	Enter the subject line that will be used in the email. You can either enter text directly, or insert a variable such as `%%SUBJECT%%`. Can be up to 250 characters. This setting is available only for email templates.	
subject-tag "<text_str>"	Enter the text to insert at the start of the subject line, such as `[NEWSLETTER]`. This setting is available only if {<email-template_name> | <message_name>} is `disclaimer-insertion`.	
subject-tag-status {enable | disable}	Enable or disable a tag in the subject line. Also configure subject-tag "<text_str>". This setting is available only if {<email-template_name> | <message_name>} is `disclaimer-insertion`.	disable
status {enable | disable}	Enable or disable prepending or appending the custom message. Also configure location {beginning | end}. This setting is available only if {<email-template_name> | <message_name>} is `disclaimer-insertion`.	disable
text-body "<text_str>"	Enter the body that will be used in the plain text format version of the email. Can be up to 4000 characters. This setting is available only for email templates.	
to <recipient_email>	Enter the recipient email address (`To:`) that will be used in the message header. You can either enter text directly, or insert a variable such as `%%ORIG_ENVELOPE_TO%%`. Can be up to 60 characters. This setting is available only for email templates.	

Related topics

domain-setting

config policy recipient

system disclaimer-message

dlp scan-rules

Use these commands to prevent sensitive data from leaving your network.

Syntax

```
config dlp scan-rules
   edit <rule_name>
         config conditions
            edit <condition_id>
               set attribute {attachment | attachment_metadata | body | body_and_attachment |
                     header | recipient | sender | sender_or_recipient | subject}
               set file-pattern {archive | audio | encrypted | executable_windows | image |
                     msoffice | openoffice | script | video}
               set group-type {local | ldap}
               set ldap-profile <profile_name>
               set operator {contain | contain_file_pattern | contain_sensitive_data | empty |
                     equal | external | internal | match | not_contain | not_equal | not_present |
                     password_protected | present}
               set sensitive-data {...}
               set value <string>
         config exceptions
            edit <exception_id>
               set attribute {attachment | attachment_metadata | body | body_and_attachment |
                     header | recipient | sender | sender_or_recipient | subject}
               set file-pattern {archive | audio | encrypted | executable_windows | image |
                     msoffice | openoffice | script | video}
               set group-type {local | ldap}
               set ldap-profile <profile_name>
               set operator {contain | contain_file_pattern | contain_sensitive_data | empty |
                     equal | external | internal | match | not_contain | not_equal | not_present |
                     password_protected | present}
               set sensitive-data {...}
               set value <string>
      set description <string>
      set condition-relation {and | or}
end
```

Variable	Description	Default
<rule_name>	Enter a descriptive name for the rule.	
description <string>	Enter a description for the DLP scan rule.	
condition-relation {and | or}	Define the relationship among conditions.	and
conditions	Configure matching or non-matching conditions to be scanned.	

Variable	Description	Default
exceptions	Configure email matching exceptions that will not be scanned.	
attribute {attachment | attachment_metadata | body | body_and_attachment | header | recipient | sender | sender_or_recipient | subject}	Select the condition/exception criteria attribute to be matched.	subject
file-pattern {archive | audio | encrypted | executable_ windows | image | msoffice | openoffice | script | video}	Enter a filename pattern to restrict fingerprinting to only those files that match the pattern.	
group-type {local | ldap}	Set whether the group is local or LDAP.	local
ldap-profile <profile_name>	Select your LDAP profile.	
operator {contain | contain_file_pattern | contain_ sensitive_data | empty | equal | external | internal | match | not_contain | not_equal | not_present | password_ protected | present}	Enter the scan conditions (for example, `contain` or `not_contain`). Options available depend on what `attribute` is set to.	contain
sensitive-data {...}	Enter a predefined sensitive information term.	
value <string>	Enter the attribute value in string format.	

domain

Use these commands to configure a protected domain.

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

Syntax

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

```
config domain
   edit <domain_name>
      config cal resource ...
      config customized-message ...
      config domain-info ...
      config domain-setting ...
      config file filter ...
      config config policy recipient ...
      config profile antispam ...
      config profile antispam-action ...
      config profile antivirus ...
      config profile antivirus-action ...
```

```
        config profile authentication ...
        config profile content ...
        config profile content-action ...
        config profile cousin-domain ...
        config profile email-address-group  ...
        config profile impersonation ...
        config profile notification ...
        config profile resource ...
        config profile user-import ...
        config config user mail ...
    next
end
```

Variable	Description	Default
<domain_name>	Type the fully qualified domain name (FQDN) of the protected domain. For example, to protect email addresses ending in "@example.com", type `example.com`.	

cal resource

Use this sub-command to configure the calendar resource of a protected domain for calendar sharing.

Syntax

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

```
config cal resource
   edit <resource_name>
      set description <string>
      set display-name <string>
      set management-users <user_email>
      set type {room | equipment}
end
```

Variable	Description	Default
<resource-name>	Enter a name for the calendar resource. This name forms the local name of the calendar resource for the current domain, for example <resource_name@<domain_name>.com.	
description <description_str>	Enter a description for the calendar resource entry.	
display-name <user_str>	Enter a display name.	
management-users <user_email>	Enter the management users for the calendar resource in the format <user_name>@<domain_name>.com.	
type {room | equipment}	Set the resource type to either room or equipment.	room

customized-message

Use this sub-command to configure the variables and the default email template of quarantine summary of a protected domain.

Syntax

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

```
config customized-message
   edit report-quarantine-summary
      config variable
         edit <name>
            set content
            set display-name
      config email-template
         edit default
            set from <string>
            set html-body <string>
            set subject <string>
            set text-body <string>
end
```

Variable	Description	Default
<name>	Enter a variable name that you want to add or edit, such as %%SENDER%%.	
content	Enter the content for the variable.	
display-name	Enter the display name for the variable. For example, the display name for %%SENDER%% can be From.	
from <string>	Enter the replacement message for the From field of the quarantine summary.	
html-body <string>	Enter the replacement message for the email body of the quarantine summary in HTML code.	
subject <string>	Enter the replacement message for the subject field of the quarantine summary.	
text-body <string>	Enter the replacement message for the email body of the quarantine summary in text format.	

domain-info

Use this sub-command to configure customer account information.

Syntax

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

```
config domain-info
```

```
    set account-limit <integer>
    set comment <string>
    set customer-email <string>
    set customer-name <string>
end
```

Variable	Description	Default
account-limit <integer>	Enter the user account limit (0 means no limit).	0
comment <string>	Optionally, enter a description.	
customer-email <string>	Enter the customer email address.	
customer-name <string>	Enter the customer name.	

domain-setting

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

Syntax

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

```
config domain-setting
   [set comment "<comment_str>"]
   set addressbook {domain | none | system}
   set bypass-bounce-verification {enable | disable}
   set disclaimer-status {disabled | use-domain-setting | use-system-setting}
   set disk-quota <GB_int>
   set dmarc-failure-action {use-policy-action | use-profile-action | use-profile-action-with-
       none | use-system-setting}
   set dmarc-report-analysis-status {enable | disable | use-system-setting}
   set dmarc-report-analysis-rua-address-mode {auto-discover | manual}
   set dmarc-report-analysis-rua-address <recipient_email>
   set dmarc-report-generation-status {enable | disable | monitor-only | use-system-setting}
   set dmarc-report-generation-from-addr-localpart <localpart_str>
   set email-continuity-status {enable | disable}
   set fallback-host {<smtp-server_fqdn> | <smtp-server_ipv4>}
   set fallback-port <port_int>
   set fallback-use-smtps {enable | disable}
   set global-bayesian {enable | disable}
   set greeting-with-host-name {domainname | hostname | othername}
   set host <host_name>
   set ip-pool <pool_name>
   set ip-pool-direction {outgoing | incoming | both}
   set is-sub-domain {enable | disable}
   set ldap-asav-profile <ldap-profile_name>
   set ldap-asav-status {enable | disable}
   set ldap-domain-routing-port <port_int>
   set ldap-domain-routing-profile <ldap-profile_name>
   set ldap-domain-routing-smtps {enable |disable}
   set ldap-groupowner-profile <ldap-profile_name>
   set ldap-routing-profile <ldap-profile_name>
   set ldap-routing-status {enable | disable}
```

```
    set ldap-user-profile <profile_name>
    set max-message-size <limit_int>
    set other-helo-greeting <hostname_str>
    set port <smtp-port_int>
    set quarantine-report-schedule-status {enable | disable}
    set quarantine-report-status {enable | disable}
    set quarantine-report-to-alt {enable | disable}
    set quarantine-report-to-alt-addr <recipient_email>
    set quarantine-report-to-individual {enable | disable}
    set quarantine-report-to-ldap-groupowner {enable | disable}
    set recipient-retention-period <days_int>
    set recipient-verification {disable | ldap | smtp}
    set recipient-verification-background {disable | ldap | purge-inactive | smtp}
    set recipient-verification-background-profile <ldap-profile_name>
    set recipient-verification-invalid-user-action {reject | discard}
    set relay-type {host | ip-pool | ldap-domain-routing | mx-lookup | mx-lookup-alt-domain}
    set remove-outgoing-received-header {enable | disable}
    set sender-addr-rate-ctrl-action
    set sender-addr-rate-ctrl-max-msgs <messages_int>
    set sender-addr-rate-ctrl-max-msgs-state {enable | disable}
    set sender-addr-rate-ctrl-max-recipients
    set sender-addr-rate-ctrl-max-recipients-state {enable | disable}
    set sender-addr-rate-ctrl-max-size <size_int>
    set sender-addr-rate-ctrl-max-size-state {enable | disable}
    set sender-addr-rate-ctrl-max-spam
    set sender-addr-rate-ctrl-max-spam-state {enable | disable}
    set sender-addr-rate-ctrl-state {enable | disable}
    set sender-addr-rate-notification-state {enable | disable}
    config sender-addr-rate-ctrl-exempt
       edit <id>
          set sender-pattern <string>
          set pattern-type {default | regexp}
    end
    set smtp-recipient-verification-command {rcpt | vrfy}
    set smtp-recipient-verification-accept-reply-string <accept_str>
    set sso-status {enable | disable}
    set sso-profile <profile_name>
    set tp-hidden {no | yes}
    set tp-server-on-port <port_int>
    set tp-use-domain-mta {yes | no}
    set use-stmps {enable | disable}
    set webmail-language <language_name>
    set webmail-theme {Blue | Dark | Green | Light-Blue | Neutrino | Red | Use-system-setting}
end
```

Variable	Description	Default
addressbook {domain | none | system}	Select whether to add newly created email users to the system address book, domain address book, or none. This setting is available only if operation-mode {gateway | server | transparent} is `server`.	domain
arc-sealing-option {all | disable | incoming | outgoing}	Select either: • `disable`:Do not sign. • `incoming`:Sign email sent between users in the same protected domain.	disable

Variable	Description	Default
	• `outgoing`:Sign email sent from a protected domain to other external or protected domains. This includes email released from quarantine. • `all`: Sign both incoming and outgoing email. This setting applies only if the ARC keys have been imported or generated.	
bypass-bounce-verification {enable | disable}	Enable to omit bounce address tag verification of email incoming to this protected domain. This bypass does not omit bounce address tagging of outgoing email.	disable
comment "<comment_str>"	Enter a description or comment.	
disclaimer-status {disabled | use-domain-setting | use-system-setting}	Select whether to use the system-wide disclaimer message (see system disclaimer-message on page 291), a disclaimer message specific to this protected domain, or to disable the disclaimer message for this protected domain. Also configure customized-message on page 87.	use-system-setting
disk-quota <GB_int>	Enter the disk quota in gigabytes (GB). If the disk quota reaches 90% threshold, a warning email is sent to the domain customer email. If the maximum disk quota of this domain is exceeded, users of this domain will no longer receive any new email. **Note:** This option is only available in server mode.	
dkim-signing-option {all | disable | incoming | outgoing}	Select either: • `disable`:Do not sign. • `incoming`:Sign email sent between users in the same protected domain. • `outgoing`:Sign email sent from a protected domain to other external or protected domains. This includes email released from quarantine. • `all`: Sign both incoming and outgoing email. This setting applies only if the DKIM keys have been imported or generated.	
dmarc-report-analysis-rua-address <recipient_email>	Enter the recipient email address where FortiMail will send the DMARC report. This setting applies only if dmarc-report-analysis-rua-address-mode {auto-discover | manual} is `manual`.	
dmarc-report-analysis-rua-address-mode {auto-discover | manual}	Select either: • `auto-discover`: FortiMail automatically queries the DNS server about the sender domain to determine that domain's authorized DMARC report recipient. **Note:** If a sender does not have a valid DMARC RUA/RUF	auto-discover

Variable	Description	Default
	configured in the domain's DNS TXT record, then FortiMail cannot send them because there is no report recipient email address. • `manual`: Manually configure another DMARC report recipient. Also configure dmarc-report-analysis-rua-address <recipient_email>. **Tip:** This option can be useful if, for example, the sender domain's DMARC record is misconfigured, and you want to send a report to show them how many email were rejected due to failed DMARC checks.	
dmarc-report-analysis-status {enable | disable | use-system-setting}	Select either: • `enable`: Collect data about email validated by DMARC checks for email sent to this protected domain. • `disable`: Do not collect DMARC check data. • `use-system-setting`: Instead of using a domain-level setting, use the system-wide setting in status {enable | disable | monitor-only} on page 45.	disable
dmarc-failure-action {use-policy-action | use-profile-action | use-profile-action-with-none | use-system-setting}	Select either: • `use-policy-action`: Use the actions specified in the `policy` option of the sender's DMARC record. • `use-profile-action`: Use the action specified in the antispam profile. • `use-profile-action-with-none`: If the policy option in the sender's DMARC record is `p=none`, use that action. Else use the action in the antispam profile. • `use-system-setting`: Instead of using a domain-level setting, use the system-wide setting dmarc-failure-action {use-policy-action | use-profile-action | use-profile-action-with-none} on page 56.	use-system
dmarc-report-generation-status {enable | disable | monitor-only | use-system-setting}	Select either: • `enable`: Send a report about email validated by DMARC checks.to the domain of the sender. • `disable`: Do not generate a DMARC report. • `monitor-only`: Do not generate a report. • `use-system-setting`: Instead of using a domain-level setting, use the system-wide setting in status {enable | disable | monitor-only} on page 45.	use-system-setting
dmarc-report-generation-from-addr-localpart <localpart_str>	Enter the local part of the sender email address when FortiMail sends reports about DMARC checks to that domain name.	noreply
fallback-host {<smtp-server_fqdn> | <smtp-server_ipv4>}	Enter the fully qualified domain name (FQDN) or IP address of the secondary SMTP server for this protected domain.	

Variable	Description	Default
	This SMTP server will be used if the primary SMTP server is unreachable. **Note:** This setting is not available in server mode.	
fallback-port <port_int>	Enter the port number on which the failover SMTP server listens. If you enable Use SMTPS, Port automatically changes to the default port number for SMTPS, but can still be customized. The default SMTP port number is 25; the default SMTPS port number is 465. **Note:** This setting is not available in server mode.	25
fallback-use-smtps {enable | disable}	Enable to use SMTPS for connections originating from or destined for this protected server. **Note:** This setting is not available in server mode.	disable
global-bayesian {enable | disable}	Enable to use the global Bayesian database instead of the Bayesian database for this protected domain. If you do not need the Bayesian database to be specific to the protected domain, you may want to use the global Bayesian database instead in order to simplify database maintenance and training. Disable to use the per-domain Bayesian database. This option does not apply if you have enabled use of personal Bayesian databases in an incoming antispam profile, and if the personal Bayesian database is mature. Instead, the FortiMail unit will use the personal Bayesian database.	disable
greeting-with-host-name {domainname | hostname | othername}	Select how the FortiMail unit will identify itself during the `HELO` or `EHLO` greeting of outgoing SMTP connections that it initiates. • `domainname`: The FortiMail unit will identify itself using the domain name for this protected domain. If the FortiMail unit will handle internal email messages (those for which both the sender and recipient addresses in the envelope contain the domain name of the protected domain), to use this option, you must also configure your protected SMTP server to use its host name for SMTP greetings. Failure to do this will result in dropped SMTP sessions, as both the FortiMail unit and the protected SMTP server will be using the same domain name when greeting each other. • `hostname`: The FortiMail unit will identify itself using its own host name. By default, the FortiMail unit uses the domain name of the protected domain. If your FortiMail unit is protecting multiple domains and using IP pool addresses, select to use the system host name instead. This setting does not apply if email is incoming, according to the sender address in the envelope, from an unprotected domain.	hostname

Variable	Description	Default
	• `othername`: Use a name other than the domain name or host name, for the `HELO`/`EHLO` greeting. Also configure other-helo-greeting <hostname_str>.	
host <host_name>	Enter the host name or IP address and port number of the mail exchanger (MX) for this protected domain. If `relay-type` is `mx-lookup` (this domain) or `mx-lookup-alt-domain` (alternative domain), this information is determined dynamically by querying the MX record of the DNS server, and this field will be empty. **Note:** This setting is not available in server mode.	
ip-pool <pool_name>	You can use a pool of IP addresses as the source IP address when sending email from this domain, or as the destination IP address when receiving email destined to this domain, or as both the source and destination IP addresses. If you want to use the IP pool as the source IP address for this protected domain, according to the sender's email address in the envelope (`MAIL FROM:`), select the IP pool to use and select `outgoing` in `ip-pool-direction {outgoing | incoming | both}`. If you want to use the IP pool as the destination IP address (virtual host) for this protected domain, according to the recipient's email address in the envelope (`RCPT TO:`), select the IP pool to use and select `incoming` in `ip-pool-direction {outgoing | incoming | both}`. You must also configure the MX record to direct email to the IP pool addresses as well. This feature can be used to support multiple virtual hosts on a single physical interface, so that different profiles can be applied to different host and logging for each host can be separated as well. If you want to use the IP pool as both the destination and source IP address, select the IP pool to use and select `both` in `ip-pool-direction {outgoing | incoming | both}`. Each email that the FortiMail unit sends will use the next IP address in the range. When the last IP address in the range is used, the next email will use the first IP address.	
ip-pool-direction {outgoing | incoming | both}	Select the direction of SMTP traffic to use an IP pool for. This setting is only available after you configure `ip-pool <pool_name>`.	
is-sub-domain {enable | disable}	Enable to indicate the protected domain you are creating is a subdomain of an existing protected domain, then also configure Main domain. Subdomains, like their parent protected domains, can be selected when configuring policies specific to that subdomain. Unlike top-level protected domains, however, subdomains will be displayed as grouped under the parent protected domain when viewing the list of protected domains.	disable

Variable	Description	Default
	This option is available only when another protected domain exists to select as the parent domain.	
ldap-asav-profile <ldap-profile_name>	Enter the name of an LDAP profile which you have enabled and configured.	
ldap-asav-status {enable | disable}	Enable to query an LDAP server for an email user's preferences to enable or disable antispam and/or antivirus processing for email messages destined for them.	disable
ldap-domain-routing-port <port_int>	Enter the port number on which the SMTP servers in the LDAP profile listen. If you enable `ldap-domain-routing-smtps {enable |disable}`, this setting automatically changes to the default port number for SMTPS, but can still be customized. The default SMTP port number is 25; the default SMTPS port number is 465. This option is valid when relay-type {host | ip-pool | ldap-domain-routing | mx-lookup | mx-lookup-alt-domain} is `ldap-domain-routing`.	25
ldap-domain-routing-profile <ldap-profile_name>	Select the name of the LDAP profile that has the FQDN or IP address of the SMTP server you want to query. Also configure ldap-domain-routing-port <port_int> and ldap-domain-routing-smtps {enable |disable}. This setting is valid when relay-type {host | ip-pool | ldap-domain-routing | mx-lookup | mx-lookup-alt-domain} is `ldap-domain-routing`.	
ldap-domain-routing-smtps {enable |disable}	Enable to use SMTPS for connections originating from or destined for this protected server. This option is valid when `relay-type {host | ip-pool | ldap-domain-routing | mx-lookup | mx-lookup-alt-domain}` is `ldap-domain-routing`.	disable
ldap-groupowner-profile <ldap-profile_name>	Select an LDAP profile to send the quarantine report to a group owner, rather than individual recipients.	
ldap-routing-profile <ldap-profile_name>	Select an LDAP profile for mail routing.	
ldap-routing-status {enable | disable}	Enable or disable mail routing according to query results from the LDAP profile.	disable
ldap-user-profile <profile_name>	Select the name of an LDAP profile in which you have configured, enabling you to authenticate email users and expand alias email addresses or replace one email address with another by using an LDAP query to retrieve alias members.	
max-message-size <limit_int>	Enable then type the limit in kilobytes (KB) of the message size. Email messages over the threshold size are rejected.	204800

Variable	Description	Default
	Note: If both this setting and its equivalent setting in the session profile are enabled, then email size will be limited to whichever size is smaller.	
other-helo-greeting <hostname_str>	After you set greeting-with-host-name {domainname | hostname | othername} to `othername`, use this command to specify the name to use for the SMTP greeting (`HELO`/`EHLO`). **Note:** This setting is not available in server mode.	
port <smtp-port_int>	Enter the SMTP port number of the mail server. **Note:** This setting is not available in server mode.	25
quarantine-report-schedule-status {enable | disable}	Enable or disable domain-level quarantine report schedule setting. The quarantine report settings for a protected domain are a subset of the system-wide quarantine report settings. For example, if the system settings for schedule include only Monday and Thursday, when you are setting the schedule for the quarantine reports of the protected domain, you will only be able to select either Monday or Thursday.	disable
quarantine-report-status {enable | disable}	Enable or disable domain-level quarantine report.	disable
quarantine-report-to-alt {enable | disable}	Enable or disable sending domain-level quarantine report to a recipient other than the individual recipients or group owner. For example, you might delegate quarantine reports by sending them to an administrator whose email address is not locally deliverable to the protected domain, such as `admin@lab.example.com`.	disable
quarantine-report-to-alt-addr <recipient_email>	Enter the email address that will receive the quarantine report.	
quarantine-report-to-individual {enable | disable}	Enable to send quarantine reports to the same email address as the original email's recipient.	enable
quarantine-report-to-ldap-groupowner {enable | disable}	Enable to send quarantine reports to the LDAP group owner, as determined by query results from the specified LDAP profile.	disable
recipient-retention-period <days_int>	Enter the retention period in days for inactive user accounts. Valid values are 15-180. If an account has been inactive for more than the designated period, the account is purged.	60
recipient-verification {disable | ldap | smtp}	Select a method of confirming that the recipient email address in the message envelope (`RCPT TO:`) corresponds to an email user account that actually exists on the protected email server. If the recipient address is invalid, the FortiMail unit will reject the email. This prevents quarantine email messages for non-existent accounts, thereby conserving quarantine hard disk space. • `disable`: Do not verify that the recipient address is an email user account that actually exists.	disable

Variable	Description	Default
	• `smtp`: Query the SMTP server using the SMTP `RCPT TO:` command to verify that the recipient address is an email user account that actually exists. You can also choose to use the SMTP `VRFY` command to do the verification. This feature is available on the GUI when you create a domain. If you want to query an SMTP server other than the one you have defined as the protected SMTP server, also enable Use alternative server, then enter the IP address or FQDN of the server in the field next to it. Also configure Port with the TCP port number on which the SMTP server listens, and enable Use SMTPS if you want to use SMTPS for recipient address verification connections with the server. • `ldap`: Query an LDAP server to verify that the recipient address is an email user account that actually exists. Also select the LDAP profile that will be used to query the LDAP server. **Note:** This option can cause a performance impact that may be noticeable during peak traffic times. For a lesser performance impact, you can alternatively periodically automatically remove quarantined email messages for invalid email user accounts, rather than actively preventing them during each email message. **Note:** Spam often contains invalid recipient addresses. If you have enabled spam quarantining, but have not prevented or scheduled the periodic removal of quarantined email messages for invalid email accounts, the FortiMail hard disk may be rapidly consumed during peak traffic times, resulting in refused SMTP connections when the hard disk becomes full. To prevent this, enable either this option or the periodic removal of invalid quarantine accounts.	
recipient-verification-background {disable | ldap | purge-inactive | smtp}	Select a method by which to periodically remove quarantined spam for which an email user account does not actually exist on the protected email server. • `disable`: Do not verify that the recipient address is an email user account that actually exists. • `ldap`: Query an LDAP server to verify that the recipient address is an email user account that actually exists. Also select the LDAP profile that will be used to query the LDAP server. If you select either Use SMTP server or Use LDAP server, at 4:00 AM daily (unless configured for another time, using the CLI), the FortiMail unit queries the server to verify the existence of email user accounts. If an email user account does not currently exist, the FortiMail unit removes all spam quarantined for that email user account. • `purge-inactive`: Checks how many days an email user account has been inactive. If an account has been inactive for more than the designated period, the account is purged. • `smtp`: Query the SMTP server to verify that the recipient address is an email user account that actually exists.	

Variable	Description	Default
	Note: If you have also enabled `recipient-verification`, the FortiMail unit is prevented from forming quarantine accounts for email user accounts that do not really exist on the protected email server. In that case, invalid quarantine accounts are never formed, and this option may not be necessary, except when you delete email user accounts on the protected email server. If this is the case, you can improve the performance of the FortiMail unit by disabling this option. **Note**: Spam often contains invalid recipient addresses. If you have enabled spam quarantining, but have not prevented or scheduled the periodic removal of quarantined email messages for invalid email accounts, the FortiMail hard disk may be rapidly consumed during peak traffic times, resulting in refused SMTP connections when the hard disk becomes full. To prevent this, enable either this option or verification of recipient addresses.	
recipient-verification-background-profile <ldap-profile_name>	Enter the LDAP profile used to query the LDAP server to verify that the recipient address is an email user account that actually exists. **Note:** This setting is not available for server mode.	
recipient-verification-invalid-user-action {reject | discard}	Select which action to take if the recipient is not valid. **Note:** This setting is not available for server mode.	reject
relay-type {host | ip-pool | ldap-domain-routing | mx-lookup | mx-lookup-alt-domain}	Select from one of the following methods of defining which SMTP server will receive email from the FortiMail unit that is destined for the protected domain: • `host`: Configure the connection to one protected SMTP server or, if any, one fallback. • `ldap-domain-routing`: Query the LDAP server for the FQDN or IP address of the SMTP server. For more information about domain lookup, see domain-query <query_str> on page 230. • `mx-lookup`: Query the DNS server's MX record of the protected domain name for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail unit will load balance between them. • `mx-lookup-alt-domain`: Query the DNS server's MX record of a domain name you specify for the FQDN or IP address of the SMTP server. If there are multiple MX records, the FortiMail unit will load balance between them. • `ip-pool`: Configure the connection to rotate among one or many protected SMTP servers. **Note:** If an MX option is used, you may also be required to configure the FortiMail unit to use a private DNS server whose MX and/or A records differ from that of a public DNS server. Requirements vary by the topology of your network and by the operating mode of the FortiMail unit.	host

Variable	Description	Default
	• **Gateway mode:** A private DNS server is required. On the private DNS server, configure the MX record with the FQDN of the SMTP server that you are protecting for this domain, causing the FortiMail unit to route email to the protected SMTP server. This is different from how a public DNS server should be configured for that domain name, where the MX record usually should contain the FQDN of the FortiMail unit itself, causing external SMTP servers to route email through the FortiMail unit. Additionally, if both the FortiMail unit and the SMTP server are behind a NAT device such as a router or firewall, on the private DNS server, configure the protected SMTP server's A record with its private IP address, while on the public DNS server, configure the FortiMail unit's A record with its public IP address. • **Transparent mode:** A private DNS server is required if both the FortiMail unit and the SMTP server are behind a NAT device such as a router or firewall. On the private DNS server, configure the protected SMTP server's A record with its private IP address. On the public DNS server, configure the protected SMTP server's A record with its public IP address. Do not modify the MX record. **Note:** This setting is not available in server mode.	
remove-outgoing-received-header {enable | disable}	Enable to remove all `Received:` message headers that have been inserted by other MTAs (not FortiMail) from email whose: • sender email address belongs to this protected domain, and • recipient email address is outgoing (that is, does not belong to this protected domain); if there are multiple recipients, only the first recipient's email address is used to determine whether an email is outgoing. Alternatively, you can remove this header from any matching email using session profiles. See remove-received-headers {enable | disable} on page 255.	disable
sender-addr-rate-ctrl-max-msgs <messages_int>	Enter the maximum number of messages per sender address per half an hour.	30
sender-addr-rate-ctrl-max-msgs-state {enable | disable}	Enable the option of maximum number of messages per sender address per half an hour.	disable
sender-addr-rate-ctrl-max-size <size_int>	Enter the maximum number of megabytes per sender per half an hour.	100
sender-addr-rate-ctrl-max-size-state {enable | disable}	Enable the option of maximum number of megabytes (MB) per sender per half an hour.	disable
sender-addr-rate-ctrl-state {enable | disable}	Enable sender address rate control per sender email address.	disable

Variable	Description	Default
smtp-recipient-verification-command {rcpt | vrfy}	Specify the command that the FortiMail unit uses to query the SMTP server to verify that the recipient address is an email user account that actually exists. The default command that the FortiMail unit uses is `RCPT TO:`. This option is only available after you set recipient-verification {disable | ldap | smtp} to `smtp`.	rcpt
smtp-recipient-verification-accept-reply-string <accept_str>	When FortiMail queries the SMTP server for recipient verification: If the reply code of the `VRFY` command is 2xx, the recipient exists. If the reply code is not 2xx, then FortiMail will try to match the accept string you specified with the reply string. If the strings match, the recipient exists. Otherwise, the recipient is unknown. For example, if the recipient is a group or mailing list, FortiMail will receive a 550 error code and a reply string. Depending on what reply string you get, you can specify a string to match the reply string. For example, if the recipient is marketing@example.com, the reply string might say something like “marketing@example.com is a group”. In this case, if you specify “is a group” as the accept string and thus this string matches the string or part of the string in the reply string, FortiMail will deem the query successful and pass the email. This command is available only when you set `smtp-recipient-verification-command` to `vrfy`. **Note:** This setting is not available in server mode.	
sso-status {enable | disable}	Enable for users in the protected domain to be able to log in via the authentication server defined in a single sign-on (SSO) profile.  When SSO is enabled for webmail users, CalDAV and WebDAV authentication will not function. They only support simple local password authentication.	disable
sso-profile <profile_name>	Enter the name of an SSO profile to use.	
tp-hidden {no | yes}	Enable to preserve the IP address or domain name of the SMTP client for incoming email messages in the: • SMTP greeting (`HELO`/`EHLO`) in the envelope • `Received:` message headers of email messages • IP addresses in the IP header This masks the existence of the FortiMail unit to the protected SMTP server. Disable to replace the SMTP client’s IP address or domain name with that of the FortiMail unit.	no

Variable	Description	Default

	For example, an external SMTP client might have the IP address 172.168.1.1, and the FortiMail unit might have the domain name fortimail.example.com. If the option is enabled, the message header would contain (difference highlighted in bold):
	`Received: from 192.168.1.1 (EHLO **172.16.1.1**) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:12:40 -0800`
	`Received: from smtpa ([172.16.1.2]) by [**172.16.1.1**] with SMTP id kAOFESEN001901 for <user1@external.example.com>; Fri, 24 Jul 2008 15:14:28 GMT`
	But if the option is disabled, the message headers would contain:
	`Received: from 192.168.1.1 (EHLO **fortimail.example.com**) (192.168.1.1) by smtp.external.example.com with SMTP; Fri, 24 Jul 2008 07:17:45 -0800`
	`Received: from smtpa ([172.16.1.2]) by **fortimail.example.com** with SMTP id kAOFJl4j002011 for <user1@external.example.com>; Fri, 24 Jul 2008 15:19:47 GMT`
	Note: This option does not apply to email messages sent from protected domains to protected domains, meaning that the FortiMail unit will not be hidden even if this option is enabled.
	Note: This setting is only available in transparent mode.	

tp-server-on-port <port_int>	Select the network interface (physical port) to which the protected SMTP server is connected. **Note:** Selecting the wrong network interface will result in the FortiMail sending email traffic to the wrong network interface. **Note:** This setting is only available in transparent mode.	0
tp-use-domain-mta {yes | no}	Enable to proxy SMTP clients' incoming connections when sending outgoing email messages via the protected SMTP server. **Note:** This option is only available in transparent mode. For example, if the protected domain example.com has the SMTP server 192.168.1.1, and an SMTP client for user1@example.com connects to it to send email to user2@external.example.net, enabling this option would cause the FortiMail unit to proxy the connection through to the protected SMTP server. Disable to relay email using the built-in MTA to either the defined SMTP relay, if any, or directly to the MTA that is the mail exchanger (MX) for the recipient email address's (`RCPT TO:`) domain. The email may not actually travel through the protected SMTP server, even though it was the relay originally specified by the SMTP client. This option does not affect incoming connections containing incoming email messages, which will always be handled by the built-in MTA. **Note:** This setting will be ignored for email that matches an antispam or content profile where you have enabled alternate-host {<relay_fqdn> | <relay_ipv4>}.	no

Variable	Description	Default
use-stmps {enable | disable}	Enable to use SMTPS to relay email to the mail server. **Note:** This setting is not available in server mode.	disable
webmail-language <language_name>	Select the language that the FortiMail unit will to display webmail and quarantine folder in the GUI for users. By default, the FortiMail unit uses the same language as the GUI for administrators.	
webmail-theme {Blue | Dark | Green | Light-Blue | Neutrino | Red | Use-system-setting}	Select a default color theme for the webmail and quarantine GUI after users log in. Alternatively, you can set this default for all protected domains (webmail-theme {Blue | Dark | Green | Light-Blue | Neutrino | Red}). If webmail-theme-status {enable | disable} is `enable`, then after they log in, each user may choose a different theme.	Use-system-setting

config policy recipient

Use this sub-command to configure a recipient-based policy for a protected domain. To configure system-wide policies, see policy recipient instead.

Syntax

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

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

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

Variable	Description	Default

profile-auth-type {imap | local | ldap | pop3 | smtp | radius}	If you want email users to be able to authenticate using an external authentication server, first specify the profile type (SMTP, POP3, IMAP,RADIUS, or LDAP), then specify which profile to use.
	For example:
	`set profile-auth-type ldap`
	`set profile-auth-ldap ldap_profile1`	

profile-auth-imap <imap_name>	Type the name of an IMAP authentication profile. This command is applicable only if you have enabled use of an IMAP authentication profile using profile-auth-type {imap | local | ldap | pop3 | smtp | radius}.	
profile-auth-ldap <ldap_name>	Type the name of an LDAP authentication profile. This command is applicable only if you have enabled use of an LDAP authentication profile using profile-auth-type {imap | local | ldap | pop3 | smtp | radius}.	
profile-auth-pop3 <pop3_name>	Type the name of a POP3 authentication profile. This command is applicable only if you have enabled use of a POP3 authentication profile using profile-auth-type {imap | local | ldap | pop3 | smtp | radius}.	
profile-auth-smtp <smtp_name>	Type the name of an SMTP authentication profile. This command is applicable only if you have enabled use of an SMTP authentication profile using profile-auth-type {imap | local | ldap | pop3 | smtp | radius}.	
profile-auth-radius <radius_name>	Type the name of a RADIUS authentication profile. This command is applicable only if you have enabled use of a RADIUS authentication profile using profile-auth-type {imap | local | ldap | pop3 | smtp | radius}.	
profile-content <profile_name>	Select which content profile you want to apply to the policy.	
profile-dlp	Enter the DLP profile for the policy.	
profile-resource <profile_name>	Select which resource profile you want to apply to the policy. This option is only available in server mode.	
profile-ldap <profile_name>	If you set the recipient type as “ldap-group", you can select an LDAP profile.	
recipient-domain <domain>	Enter the domain part of the recipient email address.	
recipient-name <name_str>	Enter the local part of the recipient email address or a pattern with wild cards.	
recipient-type {ldap-group | local-group | user}	Select one of the following ways to define recipient (`RCPT TO:`) email addresses that match this policy. This setting applies to the incoming policies only.	user

Variable	Description	Default
	`user`: Select this option and then use the above command to enter the local part of the recipient email address. `local-group`: Select this option and then specify the local group under this domain. `ldap-group`: Select this option and then select an LDAP profile.	
sender-domain <domain_name>	Enter the domain part of the sender email address. For example, example.com.	
sender-name <local-part_str>	Enter the local part of the sender email address. For example, user1.	
sender-type {ldap-group | local-group | user}	Select one of the following ways to define which sender (`MAIL FROM:`)email addresses match this policy. `user`: Select this option and then use the above command to enter the local part of the sender email address. `local-group`: Select this option and then specify the local group under this domain. `ldap-group`: Select this option and then select an LDAP profile. Note: This setting applies to the outgoing policies only.	user
smtp-diff-identity	Rejects different smtp sender identity.	
smtp-diff-identity-ldap	Verify smtp sender identity with LDAP for authenticated email.	
smtp-diff-identity-ldap-profile	LDAP profile for SMTP sender identity verification.	
status {enable | disable}	Enable or disable the policy.	enable

profile user-import

Use this command to configure account synchronization settings for remote users from LDAP and Microsoft 365 servers.

Syntax

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

```
config profile user-import
   edit <profile_name>
      set base-dn <string>
      set bind-dn <string>
      set bind-password <password>
      set description <string>
      set group-display-name <string>
      set group-primary-address <string>
```

```
      set group-query <string>
      set group-secondary-address <string>
      set ldap-port <integer>
      set ldap-secure {enable | disable}
      set ldap-server <string>
      set ldap-version {ver2 | ver3}
      set ms365-application-id <string>
      set ms365-application-secret <password>
      set ms365-tenant-id <password>
      set recurrence {daily | monthly | none | weekly}
      set referrals-chase {enable | disable}
      set schedule-hour <integer>
      set scope {base | one | sub}
      set timeout <integer>
      set type {ldap | ms365}
      set user-display-name <string>
      set user-primary-address <string>
      set user-query <string>
      set user-secondary-address <string>
   next
end
```

Variable	Description	Default
base-dn <string>	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail unit will search for user objects, such as `ou=People,dc=example,dc=com`. User objects should be child nodes of this location.	
bind-dn <string>	Enter the bind DN, such as `cn=FortiMailA,dc=example,dc=com`, of an LDAP user account with permissions to query the basedn.	
bind-password <password>	Enter the password of `bind-dn <string>`.	
description <string>	Enter a description.	
group-display-name <string>	Enter the LDAP group/mailing list display name attribute.	
group-primary-address <string>	Enter the LDAP group/mailing list primary email address attribute.	
group-query <string>	Enter the LDAP group/mailinglistquery string.	
group-secondary-address <string>	Enter the LDAP group/mailing list secondary email address attribute.	
ldap-port <integer>	Enter the TCP port number of the LDAP server. The standard port number for LDAP is 389. The standard port number for SSL-secured LDAP is 636.	389
ldap-secure {enable | disable}	Enable or disable (by default) a secure encrypted connection to the LDAP server.	disable

Variable	Description	Default
ldap-server <string>	Enter the fully qualified domain name (FQDN) or IP address of the LDAP server.	
ldap-version {ver2 | ver3}	Enter the LDAP server protocol version.	ver3
ms365-application-id <string>	Enter the Microsoft 365 application ID.	
ms365-application-secret <password>	Enter the Microsoft 365 application secret.	
ms365-tenant-id <password>	Enter the Microsoft 365 tenant ID.	
recurrence {daily | monthly | none | weekly}	Define the recurrence/schedule of the remote server synchronization.	none
referrals-chase {enable | disable}	Enable or disable (by default) chasing of referrals.	disable
schedule-hour <integer>	Enter the hour of the day at which synchronization will occur. Set the value between 0-23.	1
scope {base | one | sub}	Define the search scope of the LDAP server; either base, one level, or subtree (by default).	sub
timeout <integer>	Enter the query timeout limit in seconds. Valid range is from 60 to 600.	60
type {ldap | ms365}	Enter the remote server profile type.	ldap
user-display-name <string>	Enter the LDAP user's display name attribute.	
user-primary-address <string>	Enter the LDAP user's primary email address attribute.	
user-query <string>	Enter the LDAP query string to get all users.	
user-secondary-address <string>	Enter the LDAP user's secondary email address attribute.	

config user mail

Use this sub-command to configure email user accounts.

Syntax

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

```
config user mail
   rename <old-user_name> to <new-user_name>
   edit <user_name>
      set displayname <name_str>
      set type {ldap | ms365}
      set password <pwd_str>
      set ldap-profile <ldap_name>
   next
end
```

Variable	Description	Default
<old-user_name>	The existing user account that you want to rename.	
<new-user_name>	The new name for the user account.	
<user_name>	Enter the user name of an email user, such as `user1`. This is also the local-part of the email user's primary email address.	
type {local | ldap}	Select whether to authenticate the user via a remote authentication server, or user accounts defined locally on FortiMail.	ldap
displayname <name_str>	Enter the display name of the local email user, such as `'User One'`.	
password <pwd_str>	Enter the password of the local email user. This setting is used only if type {ldap | ms365} is `local`.	
ldap-profile <ldap_name>	Enter the name of an LDAP profile in which authentication queries are enabled. This setting is used only if type {ldap | ms365} is `ldap`.	

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

Related topics

antispam dmarc-report-generation
antispam settings
profile antispam
profile cousin-domain
profile dictionary
profile sso
profile weighted-analysis
system appearance
system fortiguard antispam

domain-association

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

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

Domain associations can be useful for saving time when you have multiple domains for which you would otherwise need to configure protected domains with identical settings.

For example, if you have one SMTP server handling email for ten domains, you could create ten separate protected domains, and configure each with identical settings. Alternatively, you could create one protected domain, listing the nine remaining domains as domain associations. The advantage of using the second method is that you do not have to repeatedly configure the same things when creating or modifying the protected domains, saving time and reducing chances for error. Changes to one protected domain automatically apply to all of its associated domains.

Alternatively, you can configure LDAP queries to automatically add domain associations. For details, see system link-monitor on page 328.

Syntax

```
config domain-association
   edit <domain-association-fqdn>
      set main-domain <protected-domain-name>
   next
end
```

Variable	Description	Default
<domain-association-fqdn>	Enter the fully qualified domain name (FQDN) of a mail domain that you want to use the same settings as the same protected domain.	
<protected-domain-name>	Enter the name of the protected domain. The associated domain will use the settings of this domain.	

Related topics

system link-monitor

file content-disarm-reconstruct

Use this command to configure content disarm and reconstruction (CDR) file attachment options.

Syntax

```
config file content-disarm-reconstruct
   set component-type-options {office-action office-dde office-embedded-object office-hyperlink
        office-linked-object office-macro pdf-action-form pdf-action-gotor pdf-action-javascript
        pdf-action-launch pdf-action-launch pdf-action-movie}
   set continue-sandbox-on-cdr {enable | disable}
   set deferred-scan-notification-option {disarm | remove}
   set deferred-scan-notification-status {enable | disable}
   set deferred-scan-verdict-option {clean | high | low | malicious | medium}
   set deferred-scan-verdict-status {enable | disable}
   set modification-notice-option {enable | disable}
end
```

Variable	Description	Default
component-type-options {office-action office-dde office-embedded-object office-hyperlink office-linked-object office-macro pdf-action-form pdf-action-gotor pdf-action-javascript pdf-action-launch pdf-action-launch pdf-action-movie}	Enter the content type(s) of attachments that you want to receive CDR. • `pdf-action-movie` • `pdf-action-sound` • `pdf-action-url` • `pdf-embedded-file` • `pdf-hyperlink` • `pdf-javascript`	
continue-sandbox-on-cdr {enable | disable}	By default, when CDR succeeds in disarming the attachment, the FortiSandbox scan is bypassed. Enable this option if you want to still perform the FortiSandbox scan, regardless of CDR result.	disable
deferred-scan-notification-option {disarm | remove}	Select whether to send notification email with a disarmed attachment, or with no attachment.	disarm
deferred-scan-notification-status {enable | disable}	Enable or disable sending the notification email on deferred scan.	disable
deferred-scan-verdict-option {clean | high | low | malicious | medium}	Determine the verdict threshold option to disarm on delivery.	clean
deferred-scan-verdict-status {enable | disable}	Enable or disable disarming the attachment of deferred email by verdict threshold.	enable

Variable	Description	Default
modification-notice-option {enable | disable}	Enable or disable appending the CDR disclaimer "Attachment has been reconstructed" for cleaned attachments.	disable

Related topics

profile content

system fortiguard url-protection

file decryption password

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

Syntax

```
config file decryption password
   edit <table_value>
      set password <string>
end
```

Variable	Description	Default
<table_value>	Enter the table value you want to add or edit.	
password <string>	Enter the password you want to use to decrypt the file.	

file filter

Use this sub-command to configure file filter options, including filtering by file extension type and Multipurpose Internet Mail Extension (MIME) type. File filters define the email attachment file types and file extensions to be scanned and are used in attachment scan rules.

Syntax

```
config file filter
   edit <filter_type>
      set description <string>
```

```
        set extension <string>
        set mime-type <string>
    end
```

Variable	Description	Default
<filter_type>	Enter the file attachment executable type to filter by.	
description <string>	Enter the description of the attachment filter.	
extension <string>	Enter an extension expressed as a wildcard, for example *.exe, or *.dll.	

mime-type <string>	Enter a MIME type in the format `<nature>/<format>`, in order to filter by file nature and format.
	For example, to filter by image, and specifically for PNG, enter the following:
	`set mime-type image/png`
	To filter for all video formats, enter the following:
	`set mime-type video/*`	

file signature

If you have hash values of some known virus-infected files, you can use this command to configure custom file signatures and then, in the antivirus profile, enable the actions against these files.

Syntax

```
config file signature
   edit <signature_name>
      [set comments "<comment_str>"]
      set source {local | remote}
      set threat-feed <feed_name>
      set type {sha1 | sha256}
      config item
         edit <hash_str>
      next
      set status {enable | disable}
   next
end
```

Variable	Description	Default
<signature_name>	Enter the file signature ID.	
comments "<comment_str>"	Enter a comment or description.	
<hash_str>	Enter the file signature hash. Use hexadecimal characters only. Valid length varies by type {sha1 | sha256}.	

Variable	Description	Default
	This setting is available only if source {local | remote} is `local`.	
source {local | remote}	Select where the file signatures are defined, either: • `local`: On the FortiMail unit. Also configure type {sha1 | sha256}. • `remote`: In a threat feed on a web server. Also configure threat-feed <feed_name>.	local
status {enable | disable}	Enable or disable the custom file signature.	enable
threat-feed <feed_name>	Enter the name of a threat feed that contains a list of hash values. This setting is available only if source {local | remote} is `remote`.	
type {sha1 | sha256}	Select the type of hash to use as the file signature. This setting is available only if source {local | remote} is `local`.	sha1

Related topics

profile antivirus

system threat-feed

log setting cloud

Use this command to configure storing log messages to the FortiAnalyzer Cloud.

Syntax

```
config log setting cloud
   set status {enable | disable} on page 113
   set loglevel {alert | critical | debug | emergency | error | information | notification |
        warning} on page 113
   set event-log-category {imap | pop3 | smtp | webmail}] on page 113
   set event-log-status {enable | disable} on page 113
   set syseventlog-category {admin | configuration | configuration-user | dns | ha | system |
        update}] on page 113
   set system-event-log-status {enable | disable} on page 114
   set antivirus-log-status {enable | disable} on page 114
   set antispam-log-status {enable | disable} on page 114
   set history-log-status {enable | disable} on page 114
   set encryption-log-status {enable | disable} on page 114
end
```

Variable	Description	Default
status {enable | disable}	Enable to send log types which are enabled to FortiAnalyzer Cloud.	enable
loglevel {alert | critical | debug | emergency | error | information | notification | warning}	Enter one of the following severity levels: • emergency • alert • critical • error • warning • notification • information • debug This log destination will receive log messages greater than or equal to this severity level. However, the relevant information level logs are always sent for any other log level selection. For details, see the FortiMail Administration Guide.	information
event-log-category {imap | pop3 | smtp | webmail}]	Enter all of the mail log types and subtypes that you want to record to this storage location. Separate each type with a space. • imap: Log all IMAP events. • pop3: Log all POP3 events. • smtp: Log all SMTP relay or proxy events. • webmail: Log all FortiMail webmail events.	webmail stmp
event-log-status {enable | disable}	Enable or disable event logging to FortiAnalyzer Cloud.	webmail smtp
syseventlog-category {admin | configuration | configuration-user | dns | ha | system | update}]	Enter all of the system event log types and subtypes that you want to record to this storage location. Separate each type with a space. • admin: Administrative events such as logins, viewing log messages, and resetting the configuration. • configuration: Configuration changes by an administrator, such as policies, profiles, and domains. • configuration-user: Configuration changes by a quarantine or webmail user, such as personal safe/block lists. • dns: DNS queries. • ha: High availability (HA) activity. • system: System events, such as rebooting the FortiMail unit or IP address configuration via DHCP. **Note**: This category does not include events from mail daemons, which are configured in event-log-category [{imap pop3 smtp webmail}].	admin configuration configuration-user dns ha system update

Variable	Description	Default
	• update: Both successful and unsuccessful attempts to download firmware and FortiGuard updates.	
system-event-log-status {enable | disable}	Enable to log system events.	enable
antivirus-log-status {enable | disable}	Enable to log all antivirus events.	enable
antispam-log-status {enable | disable}	Enable to log all antispam events.	enable
history-log-status {enable | disable}	Enable to log both successful and unsuccessful attempts by the built-in MTA or proxies to deliver email.	enable
encryption-log-status {enable | disable}	Enable to log all IBE events.	enable

log setting local

Use this command to configure log message storage on the local hard disk.

Syntax

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

Variable	Description	Default
antispam-log-status {enable | disable}	Enable to log all antispam events.	enable
antivirus-log-status {enable | disable}	Enable to log all antivirus events.	enable
disk-full {overwrite | nolog}	Enter the action the FortiMail unit will perform when the local disk is full and a new log message is caused: • `overwrite`: Delete the oldest log file in order to free disk space, and store the new log message. • `nolog`: Discard the new log message.	overwrite
encryption-log-status {enable | disable}	Enable to log all IBE events.	enable
event-log-category [{imap pop3 smtp webmail}]	Type all of the mail log types and subtypes that you want to record to this storage location. Separate each type with a space. • `imap`: Log all IMAP events. • `pop3`: Log all POP3 events. • `smtp`: Log all SMTP relay or proxy events. • `webmail`: Log all FortiMail webmail events.	webmail smtp
event-log-status {enable | disable}	Enable or disable event logging to the local hard disk.	enable
history-log-status {enable | disable}	Enable to log both successful and unsuccessful attempts by the built-in MTA or proxies to deliver email.	enable
imap-mail-log-event delete	Enable logging of delete action on email from IMAP mail client. To disable this option, enter the following command: `unset imap-mail-log-event clear`	delete
loglevel {alert | critical | debug | emergency | error | information | notification | warning}	Type one of the following severity levels: • `emergency` • `alert` • `critical` • `error` • `warning` • `notification` • `information` • `debug` This log destination will receive log messages greater than or equal to this severity level. However, the relevant information level logs are always sent for any other log level selection. For details, see the FortiMail Administration Guide.	information
pop3-mail-log-event delete	Enable logging of delete action on email from POP3 mail client. To disable this option, enter the following command: `unset pop3-mail-log-event clear`	delete

Variable	Description	Default
retention-period <days_int>	Specify how long to keep the logs. Valid range is from 1 to 1461 days. Default value is 0, which means no limit.	0
rotation-hour <hour_int>	Enter the hour of the day when the rotation should start.	0
rotation-period <days_int>	Enter the maximum age of the current log file in days. When the log file reaches either the maximum size or age, the log file is rolled (that is, the current log file is saved to a file with a new name, and a new log file is started).	10
rotation-size <file-size_int>	Enter the maximum size of the current log file in megabytes (MB). TValid range is from 1 to 500. When the log file reaches either the maximum size or age, the log file is rolled (that is, the current log file is saved to a file with a new name, and a new log file is started).	100
status {enable | disable}	Enable to send log types which are enabled to the local hard disk.	enable
syseventlog-category [{admin configuration configuration-user dns ha system update}]	Type all of the system event log types and subtypes that you want to record to this storage location. Separate each type with a space. • `admin`: Administrative events such as logins, viewing log messages, and resetting the configuration. • `configuration`: Configuration changes by an administrator, such as policies, profiles, and domains. • `configuration-user`: Configuration changes by a quarantine or webmail user, such as personal safe/block lists. • `dns`: DNS queries. • `ha`: High availability (HA) activity. • `system`: System events, such as rebooting the FortiMail unit or IP address configuration via DHCP. **Note:** This category does not include events from mail daemons, which are configured in event-log-category [{imap pop3 smtp webmail}] on page 115. • `update`: Both successful and unsuccessful attempts to download firmware and FortiGuard updates.	admin configuration configuration-user dns ha system update
system-event-log-status	Enable to log system events.	enable

Related topics

log setting remote
log alertemail recipient
log alertemail setting

log setting remote

Use this command to configure remote log message storage, either on a Syslog server or FortiAnalyzer unit.

Syntax

```
config log setting remote
   edit <log-destination_name>
      set certificate <certificate_name>
      set comma-separated-value {enable | disable}
      set comment <comment_str>
      set encryption-log-status {enable | disable}
      set event-log-category [{imap pop3 smtp webmail}]
      set event-log-status {enable | disable}
      set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kern |
        local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail |
        news | ntp}
      set hash-algorithm {sha1 |sha256}
      set history-log-status {enable | disable}
      set loglevel {alert | critical | debug | emergency | error | information | notification |
        warning}
      set matched-session-status {enable | disable}
      set name <log-destination_name>
      set port <port_int>
      set protocol {syslog | oftps}
      set reliable {enable | disable} on page 119
      set server <syslog_ipv4>
      set spam-log-status {enable | disable}
      set status {enable | disable}
      set sysevent-log-category [{admin configuration configuration-user dns ha system update}]
      set sysevent-log-status {enable | disable}
      set syslog-mode {tcp | tcp-legacy | tcp-legacy-tls | tcp-tls | udp}
      set virus-log-status {enable | disable}
end
```

Variable	Description	Default
<log-destination_name>	Enter a name to identify these remote logging settings.	
certificate <certificate_name>	Enter the name of the certificate used by TLS to encrypt the Syslog session to the remote Syslog server. This setting is available if `syslog-mode` is `tcp-tls` or `tcp-legacy-tls`.	
comma-separated-value {enable | disable}	Enable if you want to send log messages in comma-separated value (CSV) format. **Note**: Do not enable this option if the log destination is a FortiAnalyzer unit. FortiAnalyzer units do not support logs in CSV format.	disable

Variable	Description	Default
comment <comment_str>	Enter a descriptive comment.	
encryption-log-status {enable | disable}	Enable or disable IBE event logging to a remote Syslog server or FortiAnalyzer unit. See also system encryption ibe on page 295.	disable
event-log-category [{imap pop3 smtp webmail}]	Type all of the mail daemon log types and subtypes that you want to record to this storage location. Separate each type with a space. • `imap`: IMAP events. • `pop3`: POP3 events. • `smtp`: SMTP relay or proxy events. See also history-log-status {enable | disable}. • `webmail`: FortiMail webmail events.	
event-log-status {enable | disable}	Enable or disable event logging to a remote Syslog server or FortiAnalyzer unit.	disable
facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kern | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | ntp}	Type the facility identifier that the FortiMail unit will use to identify itself when sending log messages to the Syslog server. To easily identify log messages from the FortiMail unit when they are stored on the Syslog server, enter a unique facility identifier, and verify that no other network devices use the same facility identifier.	kern
hash-algorithm {sha1 |sha256}	Select the hash algorithm to use in OFTPS encryption. This setting is available if `protocol` is `oftps`.	sha1
history-log-status {enable | disable}	Enable to log both successful and unsuccessful attempts by the built-in MTA or SMTP proxy to deliver email. See also event-log-category [{imap pop3 smtp webmail}].	disable
loglevel {alert | critical | debug | emergency | error | information | notification | warning}	Type one of the following severity levels: • `emergency` • `alert` • `critical` • `error` • `warning` • `notification` • `information` • `debug` This log destination will receive log messages greater than or equal to this severity level. However, the relevant information level logs are always sent for any other log level selection. For details, see the FortiMail Administration Guide.	information
matched-session-status {enable | disable}	Enable to send only matching session logs to the remote server. Otherwise, FortiMail will send all logs. This option appears if you enabled advanced MTA control.	disable

Variable	Description	Default
name <log-destination_name>	Enter a unique name for this configuration.	
port <port_int>	If the remote host is a FortiAnalyzer unit, type `514`. If the remote host is a Syslog server, type the port number on which the Syslog server listens.	514
protocol {syslog | oftps}	Enter the protocol used to communicate with the remote log server. • `syslog`: Any compatible third-party Syslog server or FortiAnalyzer. Also configure syslog-mode {tcp | tcp-legacy | tcp-legacy-tls | tcp-tls | udp}. • `oftps`: FortiAnalyzer only. Also configure hash-algorithm {sha1 |sha256}.	syslog
reliable {enable | disable}	Reliable logging to FortiAnalyzer prevents lost logs when the connection between FortiMail and FortiAnalyzer is disrupted. When reliable mode is enabled: • Logs are cached in a FortiMail memory queue. • FortiMail sends logs to FortiAnalyzer, and FortiAnalyzer uses seq_no to track received logs. • After FortiMail sends logs to FortiAnalyzer, logs are moved to a confirm queue in FortiMail. • FortiMail periodically queries FortiAnalyzer for the latest seq_no of the last log received, and clears logs from the confirm queue up to the seq_no. • If the connection between FortiMail and FortiAnalyzer is disrupted, FortiMail resends the logs in the confirm queue to FortiAnalyzer when the connection is reestablished.	disable
server <syslog_ipv4>	Type the IPv4, IPv6, or domain name (FQDN) address of the Syslog server or FortiAnalyzer unit.	
spam-log-status {enable | disable}	Enable to log all antispam events.	disable
status {enable | disable}	Enable to send log messages to a remote Syslog server or FortiAnalyzer unit.	disable
sysevent-log-category [{admin configuration configuration-user dns ha system update}]	Type all of the system event log types and subtypes that you want to record to this storage location. Separate each type with a space. • `admin`: Administrative events such as logins and viewing log messages. • `configuration`: Configuration changes by an administrator, such as editing policies, profiles, and domains. • `configuration-user`: Configuration changes by a quarantine or webmail user, such as personal safe/block lists. • `dns`: DNS queries. • `ha`: High availability (HA) activity. • `system`: System events, such as rebooting the FortiMail unit or IP address configuration via DHCP.	

Variable	Description	Default
	Note: This category does not include events from mail daemons, which are configured in event-log-category [{imap pop3 smtp webmail}]. • `update`: Both successful and unsuccessful attempts to download firmware and FortiGuard updates.	
sysevent-log-status {enable | disable}	Enable to log system events.	disable
syslog-mode {tcp | tcp-legacy | tcp-legacy-tls | tcp-tls | udp}	Enter the transport layer protocol used for delivering the log to the remote Syslog server: • `tcp`: Slower, but more reliable than UDP: the server asks the FortiMail unit to retransmit if the server did not correctly receive the log message, compliant with RFC 6587 (Transmission of syslog Messages over TCP). **Note:** Requires that the log server supports the octet counting method. • `tcp-legacy`: TCP, but with legacy options for message delimiters instead of octet counting, compliant with RFC 3195 (Reliable Delivery for Syslog) and, for example, old versions of Kiwi Syslog Server. • `tcp-tls`: TCP, but more secure: data in the channel is encrypted during transit using TLS, compliant with RFC 5427 (Transport Layer Security Transport Mapping for Syslog). FortiMail requires that the server present a valid certificate to identify itself, and the server may also require that FortiMail unit present a valid client certificate to authenticate. Otherwise, the connection fails. Also configure certificate <certificate_name>. • `tcp-legacy-tls`: TLS, but with the same legacy options as `tcp-legacy`. • `udp`: Faster, but less reliable than TCP, and not secure: the server does not confirm if it did not correctly receive the log message, and does not encrypt log messages in transit. This setting is applicable if protocol {syslog | oftps} is `syslog`. **Caution:** Do not use UDP or TCP without encryption if logs are transmitted through untrusted networks such as the Internet. Sensitive information could be intercepted by unauthorized persons, compromising the security of your network. Use a TLS option instead. For stronger security, you can configure strong-crypto {enable | disable} and ssl-versions {ssl3 tls1_0 tls1_1 tls1_2 tls1_3}.	udp
virus-log-status {enable | disable}	Enable to log all antivirus events.	disable

Related topics

log setting local

log alertemail recipient

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

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

You must also configure which categories of events will cause the FortiMail unit to send alert email messages. For more information, see log alertemail setting on page 122.

Syntax

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

Variable	Description	Default
<recipient_email>	Type an email address that will receive alert email.	

Example

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

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

Related topics

log setting remote
log setting local
log alertemail setting

log alertemail setting

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

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

You must also configure alert email message recipients. For more information, see log alertemail recipient on page 121.

Syntax

```
config log alertemail setting
   set categories {deferq-over-limit diskfull ha license-expire remote-storage-failure system
        system-quota-full user-quota-full virus}
   set deferq-interval <interval_int>
   set deferq-trigger <trigger_int>
   set license-interval <integer>
end
```

Variable	Description	Default
categories {deferq-over-limit diskfull ha license-expire remote-storage-failure system system-quota-full user-quota-full virus}	Enter a list of one or more of the following event types that will cause alert email: • `deferq-over-limit`: The deferred mail queue has exceeded the number of messages during the interval specified in deferq-interval <interval_int> and deferq-trigger <trigger_int>. • `diskfull`: The FortiMail unit's hard disk is full. • `ha`: A high availability (HA) event such as failover has occurred. • `license-expire`: The license has expired. • `remote-storage-failure`: Email archiving to the remote host has failed. • `system`: The FortiMail unit has detected a system error. • `system-quota-full`: The FortiMail unit has reached its disk space quota. • `user-quota-full`: An email user account has reached its disk space quota. • `virus`: The FortiMail unit has detected a virus. Separate each option with a space.	system
deferq-interval <interval_int>	Enter the interval in minutes between checks of deferred queue size. This can be any number greater than zero.	30

Variable	Description	Default
deferq-trigger <trigger_int>	Enter the size that the deferred email queue must reach to cause an alert email to be sent. The valid range is 1 to 99999.	10000
license-interval <integer>	Enter the number of days (1-100) the FortiGuard license is to expire. An alert email is sent on the expiry day.	30

Related topics

log setting remote
log setting local
log alertemail recipient

mailsetting email-addr-handling

Use this command to rewrite the unqualified sender addresses -- unqualified email address is a string without @ sign, such `abc`. If this feature is enabled, the Envelope sender (`MAIL FROM:`) will be rewritten to `abc@host.domain`, while the Header `From` and `Reply-to` will be rewritten to `abc@domain`. Host is the host name attribute of the FortiMail unit and domain is the local domain name attribute of the FortiMail unit.

Set the email address (sender and recipient) parsing mode:

- Strict mode requires that the local parts of the Envelope sender (`MAIL FROM:`) and the Envelope recipient (`RCPT TO:`) strictly follow the RFC requirements.
- Relaxed mode allows non-RFC compliant local parts, such as email addresses containing multiple consecutive "." in the local parts or before "@". For example, user...name@example.com, and username...@example.com.

Syntax

```
config mailsetting email-addr-handling
   set rewrite-unqualified-sender-addr {enable | disable}
   set email-addr-parsing-mode {strict | relaxed}
end
```

Variable	Description	Default
rewrite-unqualified-sender-addr {enable | disable}	Enable or disable the unqualified email sender address rewriting feature.	disable
email-addr-parsing-mode {strict | relaxed}	Set the parsing mode to strict or relaxed.	strict

mailsetting email-continuity

Use this command to permit end users to access inbound emails when the FortiMail unit is in either Gateway or Transparent mode.

The email continuity feature is license based. This command is only available with a valid purchased license from FortiGuard, and when the FortiMail unit is operating in either Gateway or Transparent mode.

Syntax

```
config mailsetting email-continuity
   set auth-cache-period <days_int>
   set auth-cache-status {enable | disable}
   set status {enable | disable}
   set retention-period <days_int>
end
```

Variable	Description	Default
auth-cache-period <days_int>	Specify the number of days to preserve the authentication cache. The valid range is 1 to 60.	20
auth-cache-status {enable | disable}	Enable or disable authentication cache feature.	disable
retention-period <days_int>	Specify the number of days to keep emails in the folder. The valid range is 1 to 60. Note that the actual retention period is whichever is the smaller value of this setting and the `auto-delete-old-mail` sub-command under `profile resource`.	20
status {enable | disable}	Enable or disable email continuity feature.	disable

mailsetting host-mapping

Use this command to configure local host name mapping for email routing.

Syntax

```
config mailsetting host-mapping
```

```
    edit <host_name>
       set name <name_string>
       set mapped-host <host_name_string>
end
```

Variable	Description	Default
<host_name>	Emter the local host name.	
name <name_string>	Enter the name for host mapping.	
mapped-host <host_name_string>	Enter the IPaddress or host name of mapped host.	

Related topics

log setting remote
log setting local
log alertemail recipient

mailsetting mail-scan-options

Use this command to configure how FortiMail scans compressed files such as ZIP archives.

Syntax

```
config mailsetting mail-scan-options
   set content-scan-level {high | low | medium}
   set decompress-max-level <level_int>
   set decompress-max-ratio <ratio_int> on page 126
   set decompress-max-size <size_int> on page 126
   set scan-microsoft-msg {enable | disable}
   set scan-timeout-action {tempfail | passthrough}
   set scan-timeout-value <seconds_int> on page 126
end
```

Variable	Description	Default
content-scan-level {high | low | medium}	Set the scan level of dictionary and DLP rules. When set to `medium` or `high`, FortiMail uses recursive regular expressions to find a match, which consumes more system resources.	medium
decompress-max-level <level_int>	Specify how many levels to decompress the archived files for antivirus and content scan. Valid range is 1 to 36.	12

Variable	Description	Default
decompress-max-ratio <ratio_int>	Specify the maximum compression ratio for FortiMail to decompress. Valid range is 1 to 1000.	200
decompress-max-size <size_int>	Specify the maximum file size in megabytes (MB) to scan after the archived files are decompressed. This applies to every file after decompression. Bigger files will not be scanned.	10
scan-microsoft-msg {enable | disable}	Enable to scan Microsoft Transport Neutral Encapsulation format (TNEF) and MSG format attachments.	enable
scan-timeout-action {tempfail | passthrough}	When the email attachments are large and the email scanning has timed out, FortiMail can either send a temporary fail message to the sender or just let the message pass through without further scanning.	tempfail
scan-timeout-value <seconds_int>	Specify how long in seconds that FortiMail should spend on scanning email contents. Valid range is 270 to 900. When the specified timeout has been reached, FortiMail will take the action specified above.	285

Related topics

mailsetting relay-host-list
mailsetting storage central-quarantine
mailsetting storage central-quarantine
mailsetting systemquarantine

mailsetting preference

In antispam, antivirus, and content action profiles, you can select the action:

- *Deliver to alternate host*
- *Deliver to original host*
- *System quarantine*
- *Personal quarantine*
- *Disclaimer insertion*
- *Subject tag location*
- *Replacement message location*

For those actions, you can configure preferences.

Syntax

```
config mailsetting preference
   set deliver-to-alternate-host {modified_copy | unmodified_copy}
   set deliver-to-original-host {modified_copy | unmodified_copy}
   set disclaimer-insertion {selected-message | all-message}
   set domain-quarantine {modified_copy | unmodified_copy}
   set enforce-delivery {enable | disable}
   set personal-quarantine {modified_copy | unmodified_copy}
   set personal-quarantine-attachment-scan {enable | disable}
   set replacement-message-location {beginning | end}
   set subject-tag-location {beginning | end}
   set system-quarantine {modified_copy | unmodified_copy}
end
```

Variable	Description	Default
deliver-to-alternate-host {modified_copy | unmodified_copy}	For delivery and quarantine actions, you can select which form of the email to use: • `modified_copy` — Modify the email according to the action. • `unmodified_copy` — Original email header and body.  If the email is in its original form, the recipient in the SMTP envelope (`RCPT TO:`) still might be rewritten by the action. For example, when the HTML content is converted to text, if you choose to deliver the unmodified copy, then the HTML version will be delivered; if you choose to deliver the modified copy, then the plain text version will be delivered.	modified_copy
deliver-to-original-host {modified_copy | unmodified_copy}	Select to use the modified or original email.	modified_copy
disclaimer-insertion {selected-message | all-message}	Select when to insert the disclaimer: • `selected-message`: Only new email in threads. Thread replies do not receive a disclaimer. This avoids repeatedly inserting disclaimers that recipients have already seen.  Threads are detected when the same domain is in both the `Message-ID:` and `In-Reply-To:/References:` message headers. In RFC 2822, those message headers are optional. If an email client doesn't support them, then this setting has no effect. • `all-message`: Both new and reply email in threads.	selected-message

Variable	Description	Default
domain-quarantine {modified_copy | unmodified_copy}	Select to use the modified or original email.	modified_copy
enforce-delivery {enable | disable}	If the action in a profile is one of the final actions, such as system quarantine, while the action in another profile is to deliver to the original host or alternate host, you can enable this option to override the final action.	enable
personal-quarantine {modified_copy | unmodified_copy}	Select to use the modified or original email.	modified_copy
personal-quarantine-attachment-scan {enable | disable}	For spam that is sent to personal quarantine, select whether to continue or stop later scans of the email's attachments.	disable
replacement-message-location {beginning | end}	Select where to insert the attachment replacement message in the email body.	end
subject-tag-location {beginning | end}	Select to insert the tag at the start or end of the subject line.	beginning
system-quarantine {modified_copy | unmodified_copy}	Specify to use the modified email or the unmodified email.	modified_copy

Related topics

profile antispam-action

mailsetting proxy-smtp

Use this command to configure using the outgoing proxy instead of the built-in MTA for outgoing SMTP connections.

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

Syntax

```
config mailsetting proxy-smtp
   set proxy-original {enable | disable}
end
```

Variable	Description	Default
proxy-original {enable | disable}	Enable to, for outgoing SMTP connections, use the outgoing proxy instead of the built-in MTA. This allows the client to send email using the SMTP server that they specify, rather than enforcing the use of the FortiMail unit's own built-in MTA. The outgoing proxy will refuse the connection if the client's specified destination SMTP server is not available. In addition, it will not queue email from the SMTP client, and if the client does not successfully complete the connection, the outgoing proxy will simply drop the connection, and will not retry. Since authentication profiles may not successfully complete, the outgoing proxy will also ignore any authentication profiles that may be configured in the IP-based policy. The built-in MTA would normally apply authentication on behalf of the SMTP server, but the outgoing proxy will instead pass any authentication attempts through to the SMTP server, allowing it to perform its own authentication. Disable to relay email using the built-in MTA to either the SMTP relay defined in mailsetting relay-host-list on page 130, if any, or directly to the MTA that is the mail exchanger (MX) for the recipient email address's (`RCPT TO:`) domain. The email may not actually travel through the unprotected SMTP server, even though it was the relay originally specified by the SMTP client. For details, see the *FortiMail Administration Guide*. Disclaimer messages require that this option be enabled. For more information, see system disclaimer on page 290.  If this option is enabled, consider also enabling session-prevent-open-relay {enable | disable}. Failure to do so could allow clients to use open relays. **Note:** If this option is disabled, and an SMTP client is configured to authenticate, you must configure and apply an authentication profile. Without the profile, authentication with the built-in MTA will fail. Also, the mail server must be explicitly configured to allow relay from the built-in MTA in this case. **Note:** If this option is enabled, you will not be able to use IP pools. For more information, see profile ip-pool on page 220. **Note:** For security reasons, this option does not apply if there is no session profile selected in the applicable IP-based policy. For more information on configuring IP policies, see policy ip on page 151.	disable

Related topics

mailsetting relay-host-list

mailsetting storage central-quarantine

mailsetting quarantine-rescan-options

Use this command to configure quarantined mail rescan options.

Syntax

```
config mailsetting quarantine-rescan-options
   set type {antivirus | fortisandbox}
   set source {personal-quarantine | system-quarantine}
end
```

Variable	Description	Default
type {antivirus | fortisandbox}	Set the type to rescan mail either from AntiVirus or FortiSandbox.	
source {personal-quarantine | system-quarantine}	Set the source to rescan mail from either the personal quarantine or the system quarantine.	

mailsetting relay-host-list

Use this command to, if needed, configure the FortiMail unit's built-in MTA or proxy to relay outgoing mail through one or more SMTP relays.

For details such as mail relay load balancing, see the FortiMail Administration Guide.

Outgoing mail relay settings will be ignored if either:

- email matches an antispam or content profile where you have enabled `alternate-host {<relay_fqdn> | <relay_ipv4>}`
- the FortiMail unit is operating in transparent mode, and proxy-original {enable | disable} (for outgoing connections) or tp-use-domain-mta {yes | no} (for incoming connections containing outgoing email messages) is enabled.

Syntax

```
config mailsetting relay-host-list
   edit <name_str>
      set relay-type {host | ip-group | mx-lookup}
      set host-name {<mta_ipv4> | <mta_fqdn>}
```

```
    set host-port <port_int>
    set ip-group-profile <profile_name>
    set mx-lookup-domain-name <domain_str>
    set use-smtps {enable | disable}
    set auth-status {enable | disable}
    set auth-type {auto | plain | login | digest-md5 | cram-md5 | ntlm}
    set auth-username <user_str>
    set auth-password <password_str>
end
```

Variable	Description	Default
<name_str>	Enter a unique name for the entry.	
auth-password <password_str>	Enter the password of the FortiMail unit's user account on the mail relay. This setting applies if `auth-status {enable | disable}` is `enable`	
auth-status {enable | disable}	Enable this setting if the mail relay requires SMTP authentication (ESMTP `AUTH` command). Then also configure `auth-username <user_str>`, `auth-password <password_str>`, and `auth-type {auto | plain | login | digest-md5 | cram-md5 | ntlm}`.	disable
auth-type {auto | plain | login | digest-md5 | cram-md5 | ntlm}	Select the type of SMTP authentication, either: • `auto`: Automatically detect and use the most secure SMTP authentication type supported by the relay server. • `plain`: Unencrypted, scrambled password. • `login`: Unencrypted, scrambled password. • `digest-md5`: Encrypted hash of the password. • `cram-md5`: Encrypted hash of the password, with hash replay prevention, combined with a challenge and response mechanism. • `ntlm`: NT LAN Manager protocols with a hashed password. This setting applies if `auth-status {enable | disable}` is `enable`	auto
auth-username <user_str>	Enter the name of the FortiMail unit's user account on the mail relay. This setting applies if `auth-status {enable | disable}` is `enable`	
host-name {<mta_ipv4> | <mta_fqdn>}	Enter the FQDN or IP address of the mail relay. This setting applies only if `relay-type {host | ip-group | mx-lookup}` is `host`.	
host-port <port_int>	Enter the listening port number on the mail relay.	25

Variable	Description	Default
ip-group-profile <profile_name>	Enter an IP address group profile. This setting applies only if `relay-type {host | ip-group | mx-lookup}` is `ip-group`.	
mx-lookup-domain-name <domain_str>	Enter a domain name to look up its mail relays in the DNS `MX` record. This setting applies only if `relay-type {host | ip-group | mx-lookup}` is `mx-lookup`.	
relay-type {host | ip-group | mx-lookup}	Select how you will define the mail relays. • `host`: Configure the FQDN or IP address of one mail relay in `host-name {<mta_ipv4> | <mta_fqdn>}`. • `mx-lookup`: Query the DNS server's MX record of the domain name in `mx-lookup-domain-name <domain_str>` for the FQDN or IP address of the mail relays. If there are multiple MX records, each connection will randomly select one of the mail relays (also called DNS load balancing). • `ip-group`: Configure the IP addresses of the mail relays in an IP address group that you select in `ip-group-profile <profile_name>`. If there are multiple IP addresses, each connection will use the next mail relay in the group (round robin load balancing algorithm).	host
use-smtps {enable | disable}	Enable to initiate SSL- and TLS-secured connections to the mail relay if it supports SSL/TLS. When disabled, SMTP connections from the FortiMail unit's built-in MTA or proxy to the mail relay will occur as clear text, unencrypted. This option must be enabled to initiate SMTPS connections.	disable

Related topics

profile ip-address-group

system mailserver

mailsetting proxy-smtp

domain

mailsetting sender-rewriting-scheme

Configure sender rewriting scheme (SRS) settings.

SRS is used to rewrite the envelope sender of an email address, so that emails may be forwarded by an MTA if necessary without being rejected by the receiving server which may have a strict SPF policy in place.

Syntax

```
config mailsetting sender-rewriting-scheme
   config rewrite-exempt-list
      edit <domain-name>
   end
   set domain-for-rewrite {all | none | protected}
   set rewritten-addr-handling {reverse | none}
end
```

Variable	Description	Default
rewrite-exempt-list	Configure domain names that are to be exempted from sender rewriting.	
domain-for-rewrite {all | none | protected}	Select whether to rewrite external senders sending emails for all domains, for protected domains, or to not rewrite the sender at all.	none
rewritten-addr-handling {reverse | none}	For those recipients that are previously rewritten senders, set to `reverse` to reverse the recipient address and send the email to the original sender. Set to `none` to deny any recipient that is previously rewritten.	reverse

mailsetting smtp-rcpt-verification

Microsoft 365 does not accept a blank sender email address (`MAIL FROM:`) in the SMTP envelope, which is the FortiMail default setting for SMTP recipient verification. Use this command to add an envelope sender address to solve the problem.

Syntax

```
config mailsetting smtp-rcpt-verification
   set connection-type {auto | regular | secure}
   set mail-from-addr <email_str>
   set mode {regular | fail-open}
end
```

Variable	Description	Default
connection-type {auto | regular | secure}	Define the connection type for SMTP recipient verification: • `auto`: Attempt ESMTP protocol first, and fallback to SMTP protocol. ESMTP supports recipient verification for TLS-enforced back-end connections. • `regular`: Use SMTP protocol (`HELO` without `STARTTLS`). • `secure`: Use ESMTP protocol (`EHLO` with `STARTTLS`).	regular
mail-from-addr <email_str>	Enter the sender email address (`MAIL FROM:`) in the SMTP envelope.	
mode {regular | fail-open}	Define the recipient verification mode: • `regular`: Always perform recipient verification with the SMTP server. • `fail-open`: Do not perform recipient verification if the SMTP server is unreachable.	regular

mailsetting storage central-ibe

Use this command to configure storage of IBE encrypted email.

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

Syntax

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

Variable	Description	Default
remote-storage-type {disable | from-client | to-server-over-ssl}	Enter one of the following centralized IBE types: • `disable`: Centralized IBE storage is disabled. The FortiMail unit stores its IBE messages locally, on its own hard disks. • `from-client`: Select this option to allow the FortiMail unit to act as a central IBE storage server and receive IBE email from the client FortiMail units. Also configure `client-ip <client_ipv4>` for each FortiMail client. Note this feature is only available on FortiMail VM02/400E and above models. • `to-server-over-ssl`: Select this option to allow the FortiMail unit to act as a central IBE storage client and send its IBE messages to the remote FortiMail server. Also configure `server-name <name_str>` and `server-host <server_ipv4>`. All FortiMail units can act as clients.	disable

Variable	Description	Default
client-ip <client_ipv4>	This option applies only if `remote-storage-type` is set to `from-client`. Enter the IP address of the FortiMail unit that is allowed to store its IBE email on this high-end FortiMail unit. For FortiMail 1000D, 2000A, 2000B, and VM04 models, you can enter a maximum of 10 IP addresses as clients. For FortiMail 3000C and above models, you can enter a maximum of 20 IP addresses.	
server-host <server_ipv4>	This option applies only if `remote-storage-type` is set to `to-server-over-ssl`. Enter the IP address of the FortiMail unit that is acting as the central IBE storage server.	
server-name <name_str>	This option applies only if `remote-storage-type` is set to `to-server-over-ssl`. Enter the name of the FortiMail unit that is acting as the central IBE storage server. This name may be the host name or any other name that uniquely identifies the central quarantine server.	

mailsetting storage central-quarantine

Use this command to configure centralized storage of quarantined email. This command is only available on high-end models.

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

Syntax

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

Variable	Description	Default
remote-storage-type {disable | from-client | to-server-over-ssl | to-server-plain}	Enter one of the following centralized quarantine types: • `disable`: Centralized quarantine storage is disabled. The FortiMail unit stores its quarantines locally, on its own hard disks. • `from-client`: Select this option to allow the FortiMail unit to act as a central quarantine server and receive quarantined messages from other client FortiMail units. Also configure `client-ip <client_ipv4>` of the FortiMail clients. Note this feature is only available on FortiMail	disable

Variable	Description	Default
	VM02/400E and above models. • `to-server-over-ssl`: Same as `to-server-plain`, except the connection uses SSL. • `to-server-plain`: Select this option to allow the FortiMail unit to act as a central quarantine client and send quarantined messages to the remote server in plain text. Also configure `server-name <name_str>` and `server-host <server_ipv4>` of the remote server. All FortiMail units can act as clients.	
client-ip <client_ipv4>	This option applies only if `remote-storage-type` is set to `from-client`. Enter the IP address of the FortiMail unit that is allowed to store its quarantined email on this high-end FortiMail unit. For FortiMail 1000D, 2000A, 2000B, and VM04 models, you can enter a maximum of 10 IP addresses as clients. For FortiMail 3000C and above models, you can enter a maximum of 20 IP addresses.	
server-host <server_ipv4>	This option applies only if `remote-storage-type` is set to `to-server-over-ssl` or `to-server-plain`. Enter the IP address of the FortiMail unit that is acting as the central quarantine server.	
server-name <name_str>	This option applies only if `remote-storage-type` is set to `to-server-over-ssl` or `to-server-plain`. Enter the name of the FortiMail unit that is acting as the central quarantine server. This name may be the host name or any other name that uniquely identifies the central quarantine server.	

Related topics

mailsetting proxy-smtp
mailsetting relay-host-list
mailsetting storage central-quarantine
mailsetting systemquarantine
mailsetting storage central-quarantine

mailsetting storage config

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

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

Syntax

```
config mailsetting storage config
   set encryption-key
   set folder <folder_str>
   set host <host_str>
   set iscsi-id <id_str>
   set iscsi-use-initiator {enable | disable}
   set nfs-version (auto | nfs-v3 | nfs-v4}
   set password <password_str>
   set port <port_int>
   set protocol {nfs |  iscsi_server}
   set type {local | remote}
   set username <user-name_str>
end
```

Variable	Description	Default
encryption-key	Enter the key that will be used to encrypt data stored on the ISCSI server. Valid key lengths are between 6 and 64 single-byte characters. Applies only when `protocol` is `iscsi_server`.	
folder <folder_str>	Enter the directory path of the NFS export on the NAS server where the FortiMail unit will store email. Applies only when `protocol` is `nfs`.	
host <host_str>	Enter the IP address or fully qualified domain name (FQDN) of the NFS or ISCSI server.	
iscsi-id <id_str>	Enter the ISCSI identifier in the format expected by the ISCSI server, such as an ISCSI Qualified Name (IQN), Extended Unique Identifier (EUI), or T11 Network Address Authority (NAA). Applies only when `protocol` is `iscsi_server`.	
iscsi-use-initiator {enable | disable}	Enable to use ISCSI initiator name as username.	disable
nfs-version (auto | nfs-v3 | nfs-v4}	Use this command to control supported NFS versions. This command is helpful when NFS version 4 causes problems, you can specify to use NFS version 3.	auto
password <password_str>	Enter the password of the FortiMail unit's account on the ISCSI server. Applies only when `protocol` is `iscsi_server`.	
port <port_int>	Enter the TCP port number on which the NFS or ISCSI server listens for connections.	2049
protocol {nfs | iscsi_server}	Select the type of the NAS server: • `nfs`: A network file system (NFS) server. If you select this option, enter the following information: • `iscsi_server`: An Internet SCSI (Small Computer System Interface), also called iSCSI, server. If you select this option, enter the following information:	nfs

Variable	Description	Default
type {local | remote}	Select whether to store email locally or on an NFS server.	local
username <user-name_str>	Enter the user name of the FortiMail unit's account on the ISCSI server. Applies only when `protocol` is `iscsi_server`.	

Related topics

mailsetting proxy-smtp
mailsetting relay-host-list
mailsetting storage central-quarantine
mailsetting systemquarantine

mailsetting systemquarantine

Use this command to configure the system quarantine account settings.

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

Syntax

```
config mailsetting systemquarantine
   config folders
      edit <folder_name>
         set description <description>
         set retention-period <days_int>
      end
   set account <name_str>
   set forward-address <recipient_str>
   set password <password_str>
   set rotation-period <day_integer>
   set rotation-status {enable | disable}
end
```

Variable	Description	Default
description <description>	Optional description of the folder.	
retention-period <days_int>	Number of days to keep messages in the folder. The valid range is 0 to 730 (0 means no limit).	30
account <name_str>	Enter the name for the system quarantine administrator account. Surround the account name with single quotes.	systemquarantine

Variable	Description	Default
forward-address <recipient_str>	Enter an email address to which all messages diverted to the system quarantine will be copied. Surround the email address with single quotes.	
password <password_str>	Enter the password for the system quarantine administrator account. Surround the password with single quotes. The password may be entered either literally, or as a pre-encoded string prefixed with "`Enc <string>`".	forti12356net
rotation-period <day_integer>	Enter the period in days when the FortiMail unit rotates the current system quarantine folder ("Inbox"). The valid range is 1 to 90. When the folder reaches this period, the FortiMail unit renames the current folder based upon its creation date and rename date, and creates a new "Inbox" folder.	7
rotation-status {enable | disable}	Enable or disable folder rotation.	enable

Related topics

mailsetting proxy-smtp
mailsetting relay-host-list
mailsetting storage central-quarantine
mailsetting storage central-quarantine

policy access-control receive

Use this command to configure access control policies that apply to SMTP sessions being **received** by the FortiMail unit (initiated by SMTP clients).

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

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

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

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

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

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

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

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

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

See also domain on page 85.

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

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

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

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

Unlike IP-based policies, however, access control policies **cannot** affect email in ways that occur after the session's `DATA` command, such as by applying antispam profiles. Access control policies also cannot be overruled by recipient-based policies, and cannot match connections based on the SMTP server (which is always the FortiMail unit itself, **unless** the FortiMail unit is operating in transparent mode). For more information on IP-based policies, or the sequence in which access control policies are used relative to other antispam methods, see the FortiMail Administration Guide.

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

- `sender-pattern` is *
- `recipient-pattern` is *
- `authenticated` is any
- `tls-profile` is *None*
- `action` is `relay`

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

Syntax

```
config policy access-control receive
   edit <policy_name>
```

```
        [set comment "<comment_str>"]
        set action {discard | receive | reject | relay | safe | safe-relay}
        set authenticated {any | authenticated | not-authenticated}
        set recipient-pattern-type {default | external | group | internal | ldap | ldap-query |
            regexp}
        set recipient-pattern <recipient_pattern>
        set recipient-pattern-group <group_name>
        set recipient-pattern-ldap-groupname <group_name>
        set recipient-pattern-ldap-profile <profile_name>
        set reverse-dns-pattern <mta-fqdn_pattern>
        set reverse-dns-pattern-regexp {yes | no}
        set sender-ip-type {geoip-group | ip-group | ip-mask | isdb}
        set sender-geoip-group <group_name>
        set sender-ip-group <ip_group_name>
        set sender-ip-mask <sender_ipv4/mask>
        set sender-isdb {8x8 ...}
        set sender-pattern-type {default | external | group | internal | ldap | ldap-query |
            regexp}
        set sender-pattern <sender_pattern>
        set sender-pattern-group <group_name>
        set sender-pattern-ldap-groupname <group_name>
        set sender-pattern-ldap-profile <profile_name>
        set status {enable | disable}
        set tls-profile <profile_name>
end
```

Variable	Description	Default

<policy_name>	Enter the number that identifies the policy.
	Note: The identifier number may be different from the order of evaluation. FortiMail units evaluate these policies in sequential order, starting at the top of the list. Only the first matching policy is applied.
	For example, if you enter:
	`move 15 before 1`
	then policy 15 is evaluated for a match before policy 1.
	To show the order of evaluation for the list of policies, enter:
	`config policy access-control receive`
	`get`	

action {discard | receive | reject | relay | safe | safe-relay}	Select which action the FortiMail unit will perform for SMTP sessions that match this policy: • `reject`: Reject delivery of the email (SMTP reply code `550 Relaying denied`). • `discard`: Accept the email (SMTP reply code `250 OK`), but then silently delete it and do not deliver it. • `relay`: Accept the email (SMTP reply code `250 OK`), regardless of authentication or protected domain. **Do not greylist**, but continue with remaining antispam and other scans. • `safe`: Accept the email (SMTP reply code `250 OK`) if the sender authenticates or recipient belongs to a protected domain. **Greylist**, but skip remaining antispam scans. Continue other scans such as antivirus. Otherwise, if the sender does not authenticate, or the recipient does not belong to a protected domain, then reject delivery of the email (SMTP	reject

Variable	Description	Default
	reply code `554 5.7.1 Relaying denied`). In older FortiMail versions, this setting was named `bypass`. • `safe-relay`: Like `relay`, **do not greylist**, but also skip remaining antispam scans. • `receive`: Like `relay`, but **greylist**, and require authentication or protected domain. Otherwise, if the sender does not authenticate or the recipient does not belong to a protected domain, then FortiMail rejects (SMTP reply code `554 5.7.1 Relaying denied`). **Tip:**`receive` is usually used when you need to apply a TLS profile, but do not want to safelist nor allow outbound, which `relay` does. If you do **not** need to apply a TLS profile, then a policy with this action is often not required because by default, email inbound to protected domains is relayed/proxied.	
authenticated {any | authenticated | not-authenticated}	Select whether to match this policy based upon whether SMTP clients have authenticated with the FortiMail unit, either: • `any`: Ignore authentication status. • `authenticated`: Match this policy if the SMTP client has authenticated. • `not-authenticated`: Match this policy if the SMTP client has **not** authenticated.	any
comment "<comment_ str>"	Enter a description or comment. If a comment exists, it is displayed as a tool tip when you mouse-over the ID column in the list of policies in the GUI.	
recipient-pattern <recipient_ pattern>	Enter an email address or pattern. Formatting is the same as sender-pattern <sender_pattern>. This setting is available only when recipient-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `default` or `regexp`.	*
recipient-pattern-group <group_name>	Enter the group of recipient email addresses. This setting is available only if recipient-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `group`.	
recipient-pattern-ldap-groupname <group_name>	Enter the group of recipient email addresses that is in the directory server. This setting is available only if recipient-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `ldap`.	
recipient-pattern-ldap-profile <profile_ name>	Enter an LDAP profile. This setting is available only if recipient-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `ldap`. **Note**: Use `$m` in the LDAP query string to match recipient email addresses.	

Variable	Description	Default
recipient-pattern-type {default | external | group | internal | ldap | ldap-query | regexp}	Select how you will define the recipient email addresses that match the policy. Options are the same as sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp}.	default
reverse-dns-pattern <mta-fqdn_pattern>	To define which SMTP clients match this policy, depending on reverse-dns-pattern-regexp {yes | no}, enter either a: • Complete or partial domain name. Wild card characters can be used to match multiple domain names. An asterisk (*) represents one or more characters. A question mark (?) represents any single character. For example: `*.example.???` matches all sub-domains at example.com, example.net, example.org, or any other “example" domain ending with a three-letter top-level domain name. • Regular expression. **Tip:** To validate syntax and correct matching, you can use the validator in the FortiMail GUI. For details, see the FortiMail Administration Guide. Because the domain name in the SMTP session greeting (HELO/EHLO) is self-reported by the connecting SMTP client, it could be fake and the FortiMail unit does not trust it. Instead, the FortiMail does a reverse DNS lookup of the SMTP client’s IP address to discover its real domain name. This is compared to the pattern. If the domain name does not match the pattern, or if the reverse DNS query fails, then the policy does not match. **Note:** The domain name must be a valid top level domain (TLD). For example, “.lab” is not valid because it is reserved for testing on private networks, not the Internet, and thus a reverse DNS query to DNS servers on the Internet will always fail.	*
reverse-dns-pattern-regexp {yes | no}	Select yes if you want to use regular expression syntax in reverse-dns-pattern <mta-fqdn_pattern>.	no
sender-geoip-group <group_name>	Select a geographic IP address group. This setting is only available if sender-ip-type {geoip-group | ip-group | ip-mask | isdb} is `geoip-group`.	
sender-ip-group <ip_group_name>	Enter the IP group of the SMTP client attempting to send the email message. This option only appears if sender-ip-type {geoip-group | ip-group | ip-mask | isdb} is `ip-group`.	
sender-ip-mask <sender_ipv4/mask>	Enter the IP address and netmask of the SMTP client. For example, you can enter `10.10.10.10/24` to match a 24-bit subnet, or all addresses starting with 10.10.10. In the policy list, this appears as `10.10.10.0/24`, with the `0` indicating that any value is matched in that position of the address.	0.0.0.0/0

Variable	Description	Default
	Similarly, if you enter `10.10.10.10/32`, it appears as `10.10.10.10/32` because a 32-bit netmask only matches one address, 10.10.10.10 specifically. To match any address, enter `0.0.0.0/0`. This setting is only available if sender-ip-type {geoip-group | ip-group | ip-mask | isdb} is `ip-mask`.	
sender-ip-type {geoip-group | ip-group | ip-mask | isdb}	Select how you will define the source IP address of SMTP clients that match this policy, either: • `ip-mask`: An IP address and netmask. Also configure sender-ip-mask <sender_ipv4/mask>. • `ip-group`:An IP address group. Also configure sender-ip-group <ip_group_name>. • `geoip-group`: A geographic IP address group. Also configure sender-geoip-group <group_name>. • `isdb`: A service name in the Internet Service Database (ISDB) from FortiGuard. Also configure sender-isdb {8x8 ...}.	ip-mask
sender-isdb {8x8 ...}	Select a service name. The Internet Service Database (ISDB) from FortiGuard is an automatically updated list of IP addresses and subnets used by popular services such as 8x8, Akamai, Microsoft 365, and more. To display the list of options for currently known services, enter: `set sender-isdb ?` This setting is only available if sender-ip-type {geoip-group | ip-group | ip-mask | isdb} is `isdb`.	8x8
sender-pattern <sender_pattern>	Depending on your selection in sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp}: • For `default`: Enter a complete or partial email address. Wild card characters can be used to match multiple email addresses. An asterisk (*) represents one or more characters. A question mark (?) represents any single character. For example: `*@example.???` matches all email addresses at example.com, example.net, example.org, or any other “example" domain ending with a three-letter top-level domain name. • For `regexp`: Enter a regular expression. **Tip:** To validate syntax and correct matching, you can use the validator in the FortiMail GUI. For details, see the FortiMail Administration Guide. This setting is only available if sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `default` or `regexp`.	*
sender-pattern-group <group_name>	Enter the group of recipient email addresses. This setting is available only if sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `group`.	
sender-pattern-ldap-groupname <group_name>	Enter the group of recipient email addresses that is in the directory server. This setting is available only if sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `ldap`.	

Variable	Description	Default
	Note: Use `$s` in the LDAP query string to match sender email addresses.	
sender-pattern-ldap-profile <profile_name>	Enter an LDAP profile. This setting is available only if sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `ldap`.	
sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp}	Select how you will define the sender email addresses that match the policy, either: • `default`: An email address or wild card pattern that can match multiple email addresses. Also configure sender-pattern <sender_pattern>. • `external`: Email addresses that are **not** at a protected domain. • `group`: A group of email addresses configured on the FortiMail unit. Also configure sender-pattern-group <group_name>. • `internal`: Email addresses that are at a protected domain. • `ldap`: A group of email addresses configured on a directory server such as Microsoft Active Directory. Also configure sender-pattern-ldap-profile <profile_name> and sender-pattern-ldap-groupname <group_name>. • `ldap-query`: An LDAP query to a directory server such as Microsoft Active Directory. Also configure sender-pattern-ldap-profile <profile_name>. **Note**: Use `$s` in the query string to match sender addresses. For example, to reject senders that are not in the recipient's allowed sender list: **a.** Create an ACL policy and in sender-pattern-type {default \| external \| group \| internal \| ldap \| ldap-query \| regexp}, select `ldap-query`. **b.** Select an LDAP profile where this user query string is used: `&(mail=$m)(!(allowedSenders=$s)))` **c.** In action {discard \| receive \| reject \| relay \| safe \| safe-relay}, select `reject`. For each recipient (`$m`), this will match a sender (`$s`) that is not (`!`) in their `allowedSenders` list, and the action will reject it. • `regexp`: A regular expression that can match multiple email addresses. Also configure sender-pattern <sender_pattern>.	default
status {enable | disable}	Enable or disable the policy.	enable
tls-profile <profile_name>	If you want to allow or reject the connection based on whether the session attributes matches TLS profile, then select the TLS profile. • **Match:** Perform the selection in action {discard | receive | reject | relay | safe | safe-relay}. • **No Match:** Perform the selection in action {fail | tempfail} in the TLS profile.	

Related topics

profile geoip-group
policy access-control delivery
policy delivery-control
policy recipient

policy access-control delivery

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

Delivery policies can be used to encrypt each connection with TLS, and/or to encrypt each email with secure MIME (S/MIME) (also called IBE).

When the FortiMail unit initiates an SMTP session, each delivery policy is compared to the domain name in the recipient email address (`RCPT TO:`) and sender email addresses (`MAIL FROM:`) in the SMTP envelope. Policies are evaluated for a match in order, from top to bottom of the list. If a match does not exist, then the email is delivered. If a match does exist, then the connection attributes are compared to the TLS profile. Depending on the result, either the email is delivered (with encryption profile settings, if selected, and to the specified destination IP address) or the connection is not allowed. No subsequent delivery policies are applied. Only one delivery policy is ever applied to each SMTP session.

If you apply S/MIME encryption, the destination can be any email gateway or server, if either the:

- destination's MTA or mail server
- recipient's MUA

supports S/MIME and has the sender's certificate and public key, which is necessary to decrypt the email. Otherwise, the recipient cannot read the email.

Syntax

```
config policy access-control delivery
   edit <policy_name>
      set status {enable | disable}
      [set comment "<comment_str>"]
      set destination-ip-type {ip-group | ip-mask}
      set destination <destination_ipv4/mask>
      set destination-ip-group <group_name>
      set encryption-profile <profile_name>
      set ip-pool-profile <profile_name>
      set recipient-pattern-type {default | group | ldap | regexp}
      set recipient-pattern-group <group_name>
      set recipient-pattern-ldap-groupname <group_str>
      set recipient-pattern-ldap-profile <profile_name>
      set recipient-pattern <recipient_pattern>
      set sender-pattern-type {default | group | ldap | regexp}
```

```
        set sender-pattern-group <group_name>
        set sender-pattern-ldap-groupname <group_str>
        set sender-pattern-ldap-profile <profile_name>
        set sender-pattern <sender_pattern>
        set tls-profile <profile_name>
end
```

Variable	Description	Default

<policy_name>	Enter the number that identifies the policy.
	Note: The policy identifier number may be different from the order of evaluation. FortiMail units evaluate these policies in sequential order, starting at the top of the list. Only the first matching policy is applied.
	For example, if you enter:
	`move 15 before 1`
	then policy 15 is evaluated for a match before policy 1.
	To show the order of evaluation for the list of policies, enter:
	`config policy access-control delivery`
	`get`	

comment "<comment_str>"	Enter a description or comment. If a comment exists, it is displayed as a tool tip when you mouse-over the ID column in the list of policies in the GUI.	
destination <destination_ipv4/mask>	Enter an IP address and netmask. For example, enter `10.10.10.10/24` to match a 24-bit subnet, or all addresses starting with `10.10.10`. This will appear as `10.10.10.0/24` in the policy list, where the `0` at the end indicates that any value matches in that position. Similarly, `10.10.10.10/32` will appear as `10.10.10.10/32` and match only the 10.10.10.10 address. To match any address, enter `0.0.0.0/0`. This setting is available only if destination-ip-type {ip-group | ip-mask} is `ip-mask`.	0.0.0.0/0
destination-ip-group <group_name>	Enter an IP address group. This setting is available only if destination-ip-type {ip-group | ip-mask} is `ip-group`.	
destination-ip-type {ip-group | ip-mask}	If you configured tls-profile <profile_name>, then select how you will define the destination IP addresses and netmasks that match the policy, either: • `ip-group`: An IP address group. Also configure destination-ip-group <group_name>. • `ip-mask`: An IP address and netmask. Also configure destination <destination_ipv4/mask>.	ip-mask
encryption-profile <profile_name>	If you want to apply S/MIME or IBE encryption to the email, select a profile. **Note:** If you select IBE in profile content-action but S/MIME in encryption-profile <profile_name>, then IBE is overridden and not used. destination <destination_ipv4/mask> does not affect whether to apply the encryption profile.	

Variable	Description	Default
ip-pool-profile <profile_name>	Enter an IP pool profile that FortiMail will use as its source IP address when it delivers email.	
recipient-pattern <recipient_pattern>	Enter an email address or pattern. Formatting is the same as sender-pattern <sender_pattern>. This setting is available only if recipient-pattern-type {default | group | ldap | regexp} is `default` or `regexp`.	*
recipient-pattern-group <group_name>	Enter the group of recipient email addresses. This setting is available only if recipient-pattern-type {default | group | ldap | regexp} is `group`.	
recipient-pattern-ldap-groupname <group_str>	Enter the group of recipient email addresses that is in the directory server. This setting is available only if recipient-pattern-type {default | group | ldap | regexp} is `ldap`. **Note**: Use `$m` in the LDAP query string to match recipient email addresses.	
recipient-pattern-ldap-profile <profile_name>	Enter an LDAP profile. This setting is available only if recipient-pattern-type {default | group | ldap | regexp} is `ldap`.	
recipient-pattern-type {default | group | ldap | regexp}	Select how you will define the recipient email addresses that match the policy. Options are the same as sender-pattern-type {default | group | ldap | regexp}.	default
sender-pattern <sender_pattern>	Depending on your selection in sender-pattern-type {default | group | ldap | regexp}: • For `default`: Enter a complete or partial email address. Wild card characters can be used to match multiple email addresses. An asterisk (*) represents one or more characters. A question mark (?) represents any single character. For example: `*@example.???` matches all email addresses at example.com, example.net, example.org, or any other “example" domain ending with a three-letter top-level domain name. • For `regexp`: Enter a regular expression. **Tip:** To validate syntax and correct matching, you can use the validator in the FortiMail GUI. For details, see the FortiMail Administration Guide. This setting is available only if sender-pattern-type {default | group | ldap | regexp} is `default` or `regexp`.	*
sender-pattern-group <group_name>	Enter the group of recipient email addresses. This setting is available only if sender-pattern-type {default | group | ldap | regexp} is `group`.	

Variable	Description	Default
sender-pattern-ldap-groupname <group_str>	Enter the group of recipient email addresses that is in the directory server. This setting is available only if sender-pattern-type {default | group | ldap | regexp} is `ldap`. **Note**: Use `$m` in the LDAP query string to match sender email addresses.	
sender-pattern-ldap-profile <profile_name>	Enter an LDAP profile. This setting is available only if sender-pattern-type {default | group | ldap | regexp} is `ldap`.	
sender-pattern-type {default | group | ldap | regexp}	Select how you will define the sender email addresses that match the policy, either: • `default`: An email address or wild card pattern that can match multiple email addresses. Also configure sender-pattern <sender_pattern>. • `group`: A group of email addresses configured on the FortiMail unit. Also configure sender-pattern-group <group_name>. • `ldap`: A group of email addresses configured on a directory server such as Microsoft Active Directory. Also configure sender-pattern-ldap-profile <profile_name> and sender-pattern-ldap-groupname <group_str> • `regexp`: A regular expression that can match multiple email addresses. Also configure sender-pattern <sender_pattern>.	default
status {enable | disable}	Enable or disable this policy.	disable
tls-profile <profile_name>	If you want to allow or reject the connection based on whether the TLS profile matches the session, select a profile. • **Match**: Processing continues and delivery may occur. • **No match**: action {fail | tempfail} in the TLS profile occurs.	

Related topics

cloud-api profile antivirus
policy delivery-control
policy recipient
profile encryption
profile geoip-group
profile ldap
profile tls

policy delivery-control

Use this command to configure email delivery rate limits for a protected domain, or for all domains protected by the FortiMail unit. (To apply limits only for a specific sender email address instead, see sender-addr-rate-ctrl-

state {enable | disable}.)

Administrators often block MTA IP addresses that send email at a high rate because this is a common trait of spammers. Because of this, marketing mail campaigns can accidentally cause your protected domains to be registered in a DNSBL.

To prevent this problem, you can rate limit email delivery.

When the FortiMail unit initiates an SMTP session, each delivery rate limit policy is compared to the domain name in the recipient email address (`RCPT TO:`) in the SMTP envelope. Policies are evaluated for a match in order, from top to bottom of the list. If a match does not exist, then the email is delivered with no rate control. If a match does exist, then the rate limit is applied. No subsequent delivery rate limit policies are applied. Only one delivery rate limit policy is applied to each SMTP session.

Syntax

```
config policy delivery-control
   edit <policy_name>
      set max-concurrent-connection <limit_int>
      set max-messages-per-connection <limit_int>
      set max-recipients-per-message <limit_int>
      set max-recipients-per-period <limit_int>
      set recipient-domain <domain_fqdn>
      set status {enable | disable}
end
```

Variable	Description	Default

<policy_name>	Enter the number that identifies the policy.
	Note: The identifier number may be different from the order of evaluation. FortiMail units evaluate these policies in sequential order, starting at the top of the list. Only the first matching policy is applied.
	For example, if you enter:
	`move 15 before 1`
	then policy 15 is evaluated for a match before policy 1.
	To show the order of evaluation for the list of policies, enter:
	`config policy delivery-control`
	`get`	

max-concurrent-connection <limit_int>	Enter the maximum concurrent SMTP connections, or enter 0 to disable the limit. Valid range is 0-100.	5
max-messages-per-connection <limit_int>	Enter the maximum number of email per SMTP connection, or enter 0 to disable the limit. Valid range is 0-1000.	50

Variable	Description	Default
max-recipients-per-message <limit_int>	Enter the maximum recipients per email, or enter 0 to disable the limit. Valid range is 0-1000.	100
max-recipients-per-period <limit_int>	Enter the maximum recipients per 30 minute time span, or enter 0 to disable the limit. Valid range is 0-1000000000.	0
recipient-domain <domain_fqdn>	Enter a complete or partial domain name in recipient email addresses. Wild card characters can be used to match multiple domain names. An asterisk (*) represents one or more characters. A question mark (?) represents any single character. For example: `*.example.???` matches all sub-domains at example.com, example.net, example.org, or any other “example" domain ending with a three-letter top-level domain name.	*
status {enable | disable}	Enable or disable the policy.	enable

Related topics

policy access-control delivery

policy ip

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

Syntax

```
config policy ip
   edit <rule_name>
      [set comment "<comment_str>"]
      set status {enable | disable}
      set exclusive {enable | disable}
      set action {proxy-bypass | reject | scan | temp-fail}
      set source-type {geoip-group | ip-address | ip-group | isdb}
      set source-ip <client_ipv4mask>
      set source-geoip-group <group_name>
      set source-ip-group <group_name>
      set source-isdb {8x8 ...}
      set reverse-dns-pattern-regexp {no | yes}
```

```
        set reverse-dns-pattern <source_pattern>
        set destination-type {ip-address | ip-group}
        set destination-ip <smtp-server_ipv4mask>
        set destination-ip-group <group_name>
        set profile-antispam <profile_name>
        set profile-antivirus <profile_name>
        set profile-content <profile_name>
        set profile-dlp <profile_name>
        set profile-ip-pool <profile_name>
        set profile-session <profile_name>
        set profile-auth-type {imap | ldap | none | pop3 | radius | smtp}
        set profile-auth-imap <profile_name>
        set profile-auth-ldap <profile_name>
        set profile-auth-pop3 <profile_name>
        set profile-auth-radius <profile_name>
        set profile-auth-smtp <profile_name>
        set use-for-smtp-auth {enable | disable}
        set smtp-diff-identity {enable | disable}
        set smtp-diff-identity-ldap {enable | disable}
        set smtp-diff-identity-ldap-profile <profile_name>
end
```

Variable	Description	Default

<rule_name>	Enter the number that identifies the rule.
	Note: The identifier number may be different from the order of evaluation. FortiMail units evaluate policies in sequential order, starting at the top of the list. Only the first matching rule is applied.
	For example, if you enter:
	`move 15 before 1`
	then rule 15 is evaluated for a match before rule 1.
	To show the order of evaluation for the list of rules, enter:
	`config policy ip`
	`get`	

action {proxy-bypass | reject | scan | temp-fail}	Enter an action for this policy: • `proxy-bypass`: Bypass the FortiMail unit's scanning. This action is for transparent mode only. • `scan`: Accept the connection and perform any scans configured in the profiles selected in this policy. • `reject`: Reject the email and respond to the SMTP client with SMTP reply code 550, indicating a permanent failure. • `temp-fail`: Reject the email and respond to the SMTP client with SMTP reply code 451, indicating and indicate a temporary failure.	scan
destination-ip-group <group_name>	Enter the name of the IP group of the SMTP servers. This option is only available when the destination-type {ip-address | ip-group} is `ip-group`.	
destination-ip <smtp-server_ipv4mask>	Enter the IP address and subnet mask of the SMTP server. To match all servers, enter `0.0.0.0/0`.	0.0.0.0 0.0.0.0

Variable	Description	Default
	This option applies only for FortiMail units operating in transparent mode. For other modes, the FortiMail unit receives the SMTP connection, and therefore acts as the server.	
destination-type {ip-address | ip-group}	Select how you will define the destination IP address of the SMTP servers whose connections will match this policy. Also configure destination-ip <smtp-server_ipv4mask>, destination-ip-group <group_name>.	ip-address
source-isdb {8x8 ...}	Select a service name. The Internet Service Database (ISDB) is an automatically updated list of IP addresses and subnets used by popular services such as 8x8, Akamai, Microsoft 365, and more. To display the list of options for currently known services, enter: `set sender-isdb ?` This setting is only available if source-type {geoip-group | ip-address | ip-group | isdb} is `isdb`.	
source-geoip-group <group_name>	Enter the geographic IP group of the SMTP clients. This setting is only available if source-type {geoip-group | ip-address | ip-group | isdb} is `geoip-group`.	
source-ip-group <group_name>	Enter the IP group of the SMTP clients. This setting is only available if source-type {geoip-group | ip-address | ip-group | isdb} is `ip-group`.	
source-ip <client_ipv4mask>	Enter the IP address and subnet mask of the SMTP client. To match all clients, enter `0.0.0.0/0`.	192.168.224.15 255.255.255.255
source-type {geoip-group | ip-address | ip-group | isdb}	Select how you will define the source IP address of the SMTP clients whose connections will match this policy. Then configure the related setting such as source-isdb {8x8 ...}.	ip-address
comment "<comment_str>"	Enter a description or comment.	
exclusive {enable | disable}	Enable to omit evaluation of matches with recipient-based policies, causing the FortiMail unit to disregard applicable recipient-based policies and apply only the IP-based policy. Disable to apply both the matching recipient-based policy and IP-based policy. Any profiles selected in the recipient-based policy will override those selected in the IP-based policy.	disable
profile-antispam <profile_name>	Enter the name of an outgoing antispam profile, if any, that this policy will apply.	

Variable	Description	Default
profile-antivirus <profile_name>	Enter the name of an antivirus profile, if any, that this policy will apply.	
profile-auth-imap <profile_name>	Enter the name of an IMAP authentication profile. This setting applies if profile-auth-type {imap | ldap | none | pop3 | radius | smtp} is `imap`.	
profile-auth-ldap <profile_name>	Enter the name of an LDAP authentication profile. This setting applies if profile-auth-type {imap | ldap | none | pop3 | radius | smtp} is `ldap`.	
profile-auth-pop3 <profile_name>	Enter the name of a POP3 authentication profile. This setting applies if profile-auth-type {imap | ldap | none | pop3 | radius | smtp} is `pop3`.	
profile-auth-radius <profile_name>	Enter the name of a RADIUS authentication profile. This setting applies if profile-auth-type {imap | ldap | none | pop3 | radius | smtp} is `radius`.	
profile-auth-smtp <profile_name>	Enter the name of an SMTP authentication profile. This setting applies if profile-auth-type {imap | ldap | none | pop3 | radius | smtp} is `smtp`.	
profile-auth-type {imap | ldap | none | pop3 | radius | smtp}	Select the type of the authentication profile that this policy will apply, or select `none` if you do not want to apply authentication. Also configure the name of the profile in profile-auth-ldap <profile_name> etc.	none
profile-content <profile_name>	Enter the name of the content profile that you want to apply to connections matching the policy.	
profile-dlp <profile_name>	Enter the name of the DLP profile that you want to apply to connections matching this policy.	
profile-ip-pool <profile_name>	Enter the name of the IP pool profile that you want to apply to connections matching the policy.	
profile-session <profile_name>	Enter the name of the session profile that you want to apply to connections matching the policy.	

Variable	Description	Default
reverse-dns-pattern <source_pattern>	To define which SMTP clients match this policy, depending on reverse-dns-pattern-regexp {no | yes}, enter either a: • Complete or partial domain name. Wild card characters can be used to match multiple domain names. An asterisk (*) represents one or more characters. A question mark (?) represents any single character. For example: `*.example.???` matches all sub-domains at example.com, example.net, example.org, or any other “example" domain ending with a three-letter top-level domain name. • Regular expression. **Tip:** To verify syntax and correct matching, use the validator in the GUI. See also regular expression syntax in the FortiMail Administration Guide. Because the domain name in the SMTP session greeting (`HELO`/`EHLO`) is self-reported by the connecting SMTP client, it could be fake and the FortiMail unit does not trust it. Instead, the FortiMail does a reverse DNS lookup of the SMTP client’s IP address to discover its real domain name. This is compared to the pattern. If the domain name does not match the pattern, or if the reverse DNS query fails, then the policy does not match. **Note:** The domain name must be a valid top level domain (TLD). For example, `.lab` is not valid because it is reserved for testing on RFC 1918 **private** networks, not the Internet, and thus a reverse DNS query to **public** DNS servers on the Internet will always fail.	*
reverse-dns-pattern-regexp {no | yes}	Select whether the pattern that you enter in reverse-dns-pattern <source_pattern> will be interpreted as a regular expression.	no
smtp-diff-identity {enable | disable}	Enable to allow the SMTP client to send email using a different sender email address (`MAIL FROM:`) than the user name that they used to authenticate. Disable to require that the sender email address in the SMTP envelope match the authenticated user name. **Caution:** If smtp-eom-bare-lf-handling {allow | disallow | ignore} is `ignore`, then multiple email with different senders could be in the message body. To prevent impersonation, set this setting to `disable`.	disable
smtp-diff-identity-ldap {enable | disable}	Enable or disable whether to verify the sender's identity with LDAP authentication.	disable

Variable	Description	Default
smtp-diff-identity-ldap-profile <profile_name>	Enter the name of the LDAP profile to use for SMTP sender identity verification. This setting is only available if smtp-diff-identity-ldap {enable | disable} is enable.	disable
status {enable | disable}	Enable or disable the policy.	enable
use-for-smtp-auth {enable | disable}	Enable to authenticate SMTP connections using the authentication profile configured in sensitive-data {...}.	disable

Related topics

cloud-api profile antivirus
policy access-control delivery
policy access-control receive
policy recipient
profile geoip-group

policy recipient

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

Syntax

```
config policy recipient
   edit <policy_int>
      [set comment "<comment_str>"
      set status {enable | disable}
      set direction {incoming | outgoing}
      set recipient-type {email-user-group | import-group | import-user | ldap-group | user-
          regex | user-wildcard}
      set recipient-name <local-part_str>
      set recipient-domain <domain_str>
      set recipient-email-address-group <group_name>
      set profile-ldap-recipient <ldap-profile_name>
      set recipient-regex <recipient_pattern>
      set recipient-exclusion-status {enable | disable}
      set recipient-exclusion-type {email-address-group | user-regex | user-wildcard}
      set recipient-exclusion-email-address-group <group_name>
```

```
        set recipient-exclusion-name <local-part-str>
        set recipient-exclusion-domain <domain-part_str>
        set recipient-exclusion-regex <exclusion_pattern>
        set sender-type {email-user-group | import-group | import-user | ldap-group | user-regex |
          user-wildcard}
        set sender-name <local-part_str>
        set sender-domain <domain_str>
        set sender-email-address-group <group_name>
        set profile-ldap-sender <ldap-profile_name>
        set sender-regex <sender_pattern>
        set smtp-diff-identity {enable | disable}
        set smtp-diff-identity-ldap {enable | disable}
        set smtp-diff-identity-ldap-profile <profile_name>
        set auth-access-options {pop3 | smtp-auth | smtp-diff-identity | web}
        set pkiauth {enable | disable}
        set pkiuser <user_str>
        set certificate-required {yes | no}
        set profile-auth-type {imap | ldap | local | none | pop3 | radius | smtp}
        set profile-antispam <antispam-profile_name>
        set profile-antivirus <antivirus-profile_name>
        set profile-content <content-profile_name>
        set profile-dlp <profile_name>
        set profile-resource <profile_name>
end
```

Variable	Description	Default
<policy_int>	Enter the index number of the recipient-based policy.	
auth-access-options {pop3 | smtp-auth | smtp-diff-identity | web}	Enter the method that email users matching this policy use to retrieve the contents of their per-recipient spam quarantine. • `pop3`: Allow the email user to use POP3 to retrieve the contents of their per-recipient spam quarantine. • `smtp-auth`: Use the authentication server selected in the authentication profile when performing SMTP authentication for connecting SMTP clients. • `smtp-diff-identity`: Allow email when the SMTP client authenticates with a different user name than the one that appears in the envelope's sender email address. You must also enter `smtp-auth` for this option to have any effect. • `web`: Allow the email user to use FortiMail webmail (HTTP or HTTPS) to retrieve the contents of their per-recipient spam quarantine. **Note:** Entering this option allows, but does not require, SMTP authentication. To enforce SMTP authentication for connecting SMTP clients, ensure that all access control rules require authentication.	
certificate-required {yes | no}	If the email user's web browser does not provide a valid personal certificate, the FortiMail unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enter `yes`. This setting only applies if pkiauth {enable | disable} is `enable`.	no

Variable	Description	Default
comment "<comment_str>"	Enter a comment or description.	
direction {incoming | outgoing}	Select the direction of email traffic that this policy matches.	incoming
pkiauth {enable | disable}	Enable if you want to allow email users to log in to their per-recipient spam quarantine by presenting a certificate rather than a user name and password. Also configure pkiuser <user_str> and `certificate-required {yes | no}`.	disable
pkiuser <user_str>	Enter the name of a PKI user, such as `user1`. This setting only applies if pkiauth {enable | disable} is `enable`. Also configure `config user pki`.	
profile-antispam <antispam-profile_name>	Enter the name of an antispam profile, if any, that this policy will apply.	
profile-antivirus <antivirus-profile_name>	Enter the name of an antivirus profile, if any, that this policy will apply.	
profile-auth-type {imap | ldap | local | none | pop3 | radius | smtp}	Enter the type of the authentication profile that this policy will apply. Depending on the type that you select, also configure profile-auth-imap <profile_name> etc.	none
profile-auth-imap <profile_name>	Select the name of a profile to use for authentication. This setting is available only if profile-auth-type {imap | ldap | local | none | pop3 | radius | smtp} is `imap`.	
profile-auth-ldap <profile_name>	Select the name of a profile to use for authentication. This setting is available only if profile-auth-type {imap | ldap | local | none | pop3 | radius | smtp} is `ldap`.	
profile-auth-pop3 <profile_name>	Select the name of a profile to use for authentication. This setting is available only if profile-auth-type {imap | ldap | local | none | pop3 | radius | smtp} is `pop3`.	
profile-auth-radius<profile_name>	Select the name of a profile to use for authentication. This setting is available only if profile-auth-type {imap | ldap | local | none | pop3 | radius | smtp} is `radius`.	
profile-auth-smtp <profile_name>	Select the name of a profile to use for authentication. This setting is available only if profile-auth-type {imap | ldap | local | none | pop3 | radius | smtp} is `smtp`.	
profile-dlp <profile_name>	Enter the name of the DLP profile that you want to apply to connections matching the policy.	
profile-content <content-profile_name>	Enter the name of the content profile that you want to apply to connections matching the policy.	
profile-resource <profile_name>	Enter the name of the resource profile that you want to apply to connections matching the policy.	

Variable	Description	Default
profile-ldap-recipient <ldap-profile_name>	If recipient-type {email-user-group | import-group | import-user | ldap-group | user-regex | user-wildcard} is `ldap-group`, enter the name of an LDAP profile in which the group owner query has been enabled and configured.	
profile-ldap-sender <ldap-profile_name>	If sender-type {email-user-group | import-group | import-user | ldap-group | user-regex | user-wildcard} is `ldap-group`, enter the name of an LDAP profile in which the group owner query has been enabled and configured.	
recipient-domain <domain_str>	Enter the domain name of recipient email addresses that match this policy.	
recipient-email-address-group <group_name>	Enter the group of recipient email addresses. This setting is available only if recipient-type {email-user-group | import-group | import-user | ldap-group | user-regex | user-wildcard} is `email-user-group`.	
recipient-exclusion-domain <domain-part_str>	Enter the domain name of recipient email addresses that you want to exclude. This setting is available only if recipient-exclusion-type {email-address-group | user-regex | user-wildcard} is `user-wildcard`.	*
recipient-exclusion-email-address-group <group_name>	Select a group of email addresses you want to exclude. This setting is available only if recipient-exclusion-type {email-address-group | user-regex | user-wildcard} is `email-address-group`.	
recipient-exclusion-name <local-part-str>	Enter the local part (username) of recipient email addresses that you want to exclude. This setting is available only if recipient-exclusion-type {email-address-group | user-regex | user-wildcard} is `user-wildcard`.	*
recipient-exclusion-regex <exclusion_pattern>	Enter a regular expression that matches only recipient email addresses that you want to exclude. This setting is available only if recipient-exclusion-type {email-address-group | user-regex | user-wildcard} is `user-regex`.	
recipient-exclusion-status {enable | disable}	Enable if you want to exclude some recipient email addresses from matching this policy.	disable
recipient-exclusion-type {email-address-group | user-regex | user-wildcard}	Select how you want to define excluded recipient email addresses. Depending on which you select, also configure recipient-exclusion-name <local-part-str> etc. This setting is available only if recipient-exclusion-status {enable | disable} is `enable`.	user-wildcard
recipient-name <local-part_str>	Enter the local part (username) of recipient email addresses that match this policy.	
recipient-regex <recipient_pattern>	Enter a regular expression that matches only the recipient email addresses that should match this policy.	.*

Variable	Description	Default
	This setting is only available when recipient-type {email-user-group | import-group | import-user | ldap-group | user-regex | user-wildcard} is `regexp`.	
recipient-type {email-user-group | import-group | import-user | ldap-group | user-regex | user-wildcard}	Enter one of the following ways to define recipient (`RCPT TO:`) email addresses that match this policy. Depending on which you select, also configure profile-ldap-recipient <ldap-profile_name>, recipient-regex <recipient_pattern>, etc.	user
sender-domain <domain_str>	Enter the domain name of sender email addresses that match this policy. This setting is available only if sender-type {email-user-group | import-group | import-user | ldap-group | user-regex | user-wildcard} is `user-wildcard`.	
sender-email-address-group <group_name>	Enter the group of sender email addresses. This setting is available only if sender-type {email-user-group | import-group | import-user | ldap-group | user-regex | user-wildcard} is `email-user-group`.	
sender-name <local-part_str>	Enter the local part (username) of sender email addresses that match this policy. This setting is available only if sender-type {email-user-group | import-group | import-user | ldap-group | user-regex | user-wildcard} is `user-wildcard`.	
sender-regex <sender_pattern>	Enter a regular expression that matches only the sender email addresses that should match this policy. This setting is only available when sender-type {email-user-group | import-group | import-user | ldap-group | user-regex | user-wildcard} is `regexp`.	.*
sender-type {email-user-group | import-group | import-user | ldap-group | user-regex | user-wildcard}	Select how to define sender (`MAIL FROM:`) email addresses that match this policy. Depending on which you select, also configure profile-ldap-sender <ldap-profile_name>, sender-regex <sender_pattern>, etc.	user
smtp-diff-identity {enable | disable}	Enable to allow the SMTP client to send email using a different sender email address (`MAIL FROM:`) than the user name that they used to authenticate. Disable to require that the sender email address in the SMTP envelope match the authenticated user name. This setting is applicable only if `smtp auth` is used.	enable
smtp-diff-identity-ldap {enable | disable}	Enable to allow the SMTP client to verify SMTP sender identity with LDAP for authenticated email. This setting is applicable only if `smtp auth` is used.	disable
smtp-diff-identity-ldap-profile <profile_name>	Enter the LDAP profile name for SMTP sender identity verification. This setting is applicable only if `smtp auth` is used.	

Variable	Description	Default
status {enable | disable}	Enable to apply this policy.	enable

Related topics

cloud-api profile antivirus
policy access-control delivery
policy delivery-control
profile antispam
profile antivirus
profile content
profile dlp
profile email-address-group
profile ldap
profile resource
user pki

profile access-control

Use this command to configure access control profiles. These profiles have settings like policy access-control delivery and policy access-control receive, but can be used via session profiles instead.

This feature is available if you have the advanced MTA feature license, and have enabled the feature in mta-adv-ctrl-status {enable | disable}.

Syntax

```
config profile access-control
   edit <profile_name>
      [set comment "<comment_str>"]
      config access-control
         edit <policy_name>
            set action {discard | receive | reject | relay | safe | safe-relay}
            set authenticated {any | authenticated | not-authenticated}
            set recipient-pattern-type {default | external | group | internal | ldap | ldap-query |
                regexp}
            set recipient-pattern <recipient_pattern>
            set recipient-pattern-group <group_name>
            set recipient-pattern-ldap-profile <profile_name>
            set recipient-pattern-group <group_name>
            set reverse-dns-pattern <mta-fqdn_pattern>
            set reverse-dns-pattern-regexp {yes | no}
            set sender-ip-type {geoip-group | ip-group | ip-mask}
```

```
            set sender-ip-mask <sender_ipv4/mask>
            set sender-pattern-type {default | external | group | internal | ldap | ldap-query |
                regexp}
            set sender-pattern <sender_pattern>
            set sender-pattern-group <group_name>
            set sender-pattern-ldap-groupname <group_name>
            set sender-pattern-ldap-profile <profile_name>
            set status {enable | disable}
            set tls-profile <profile_name>
        end
end
```

Variable	Description	Default
<profile_name>	Enter the name that identifies the profile.	
comment "<comment_str>"	Enter a description or comment.	

<policy_name>	Enter the number that identifies the policy.
	Note: The identifier number may be different from the order of evaluation. FortiMail units evaluate these policies in sequential order, starting at the top of the list. Only the first matching policy is applied.
	For example, if you enter:
	`move 15 before 1`
	then policy 15 is evaluated for a match before policy 1.
	To show the order of evaluation for the list of policies, enter:
	`get`	

action {discard | receive | reject | relay | safe | safe-relay}	Select which action the FortiMail unit will perform for SMTP sessions that match this policy: • `reject`: Reject delivery of the email (SMTP reply code `550 Relaying denied`). • `discard`: Accept the email (SMTP reply code `250 OK`), but then silently delete it and do not deliver it. • `relay`: Accept the email (SMTP reply code `250 OK`), regardless of authentication or protected domain. **Do not greylist**, but continue with remaining antispam and other scans. • `safe`: Accept the email (SMTP reply code `250 OK`) if the sender authenticates or recipient belongs to a protected domain. **Greylist**, but skip remaining antispam scans. Continue other scans such as antivirus. Otherwise, if the sender does not authenticate, or the recipient does not belong to a protected domain, then reject delivery of the email (SMTP reply code `554 5.7.1 Relaying denied`). In older FortiMail versions, this setting was named `bypass`. • `safe-relay`: Like `relay`, **do not greylist**, but also skip remaining antispam scans. • `receive`: Like `relay`, but **greylist**, and require authentication or protected domain. Otherwise, if the sender does not authenticate or the recipient does not	reject

Variable	Description	Default
	belong to a protected domain, then FortiMail rejects (SMTP reply code `554 5.7.1 Relaying denied`). **Tip:** `receive` is usually used when you need to apply a TLS profile, but do not want to safelist nor allow outbound, which `relay` does. If you do **not** need to apply a TLS profile, then a policy with this action is often not required because by default, email inbound to protected domains is relayed/proxied.	
authenticated {any | authenticated | not-authenticated}	Select whether to match this policy based upon whether SMTP clients have authenticated with the FortiMail unit, either: • `any`: Ignore authentication status. • `authenticated`: Match this policy if the SMTP client has authenticated. • `not-authenticated`: Match this policy if the SMTP client has **not** authenticated.	any
recipient-pattern <recipient_pattern>	Enter an email address or pattern. Formatting is the same as sender-pattern <sender_pattern>. This setting is available only when recipient-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `default` or `regexp`.	*
recipient-pattern-group <group_name>	Enter the group of recipient email addresses. This setting is available only if recipient-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `group`.	
recipient-pattern-ldap-groupname <group_name>	Enter the group of recipient email addresses that is in the directory server. This setting is available only if recipient-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `ldap`.	
recipient-pattern-ldap-profile <profile_name>	Enter an LDAP profile. This setting is available only if recipient-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `ldap`. **Note**: Use `$m` in the LDAP query string to match recipient email addresses.	
recipient-pattern-type {default | external | group | internal | ldap | ldap-query | regexp}	Select how you will define the recipient email addresses that match the policy. Options are the same as sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp}.	default
reverse-dns-pattern <mta-fqdn_pattern>	To define which SMTP clients match this policy, depending on reverse-dns-pattern-regexp {yes | no}, enter either a: • Complete or partial domain name. Wild card characters can be used to match multiple domain names. An asterisk (*) represents one or more characters. A question mark (?) represents any single character. For example: `*.example.???` matches all sub-domains at example.com, example.net, example.org, or	*

Variable	Description	Default
	any other “example" domain ending with a three-letter top-level domain name. • Regular expression. **Tip:** To validate syntax and correct matching, you can use the validator in the FortiMail GUI. For details, see the FortiMail Administration Guide. Because the domain name in the SMTP session greeting (`HELO/EHLO`) is self-reported by the connecting SMTP client, it could be fake and the FortiMail unit does not trust it. Instead, the FortiMail does a reverse DNS lookup of the SMTP client’s IP address to discover its real domain name. This is compared to the pattern. If the domain name does not match the pattern, or if the reverse DNS query fails, then the policy does not match. **Note:** The domain name must be a valid top level domain (TLD). For example, “.lab” is not valid because it is reserved for testing on private networks, not the Internet, and thus a reverse DNS query to DNS servers on the Internet will always fail.	
reverse-dns-pattern-regexp {yes | no}	Select `yes` if you want to use regular expression syntax in reverse-dns-pattern <mta-fqdn_pattern>.	no
sender-geoip-group <group_name>	Select a geographic IP address group. This setting is only available if sender-ip-type {geoip-group | ip-group | ip-mask} is `geoip-group`.	
sender-ip-group <ip_group_name>	Enter the IP group of the SMTP client attempting to send the email message. This setting is only available if sender-ip-type {geoip-group | ip-group | ip-mask} is `ip-group`.	
sender-ip-mask <sender_ipv4/mask>	Enter the IP address and netmask of the SMTP client. For example, you can enter `10.10.10.10/24` to match a 24-bit subnet, or all addresses starting with 10.10.10. In the access control policy table, this appears as `10.10.10.0/24`, with the `0` indicating that any value is matched in that position of the address. Similarly, if you enter `10.10.10.10/32`, it appears as `10.10.10.10/32` because a 32-bit netmask only matches one address, 10.10.10.10 specifically. To match any address, enter `0.0.0.0/0`. This setting is only available if sender-ip-type {geoip-group | ip-group | ip-mask} is `ip-mask`.	0.0.0.0/0
sender-ip-type {geoip-group | ip-group | ip-mask}	Select how you will define the source IP address of SMTP clients that match this policy, either: • `ip-mask`: An IP address and netmask. Also configure sender-ip-mask <sender_ipv4/mask>. • `ip-group`:An IP address group. Also configure sender-ip-group <ip_group_name>. • `geoip-group`: A geographic IP address group. Also configure sender-geoip-group <group_name>. • `isdb`: A service name in the Internet Service Database (ISDB) from	ip-mask

Variable	Description	Default
	FortiGuard. Also configure sender-isdb {8x8 ...}.	
sender-isdb {8x8 ...}	Select a service name. The Internet Service Database (ISDB) from FortiGuard is an automatically updated list of IP addresses and subnets used by popular services such as 8x8, Akamai, Microsoft 365, and more. To display the list of options for currently known services, enter: `set sender-isdb ?` This setting is only available if sender-ip-type {geoip-group | ip-group | ip-mask} is `isdb`.	8x8
sender-pattern <sender_pattern>	Depending on your selection in sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp}: • For `default`: Enter a complete or partial email address. Wild card characters can be used to match multiple email addresses. An asterisk (*) represents one or more characters. A question mark (?) represents any single character. For example: `*@example.???` matches all email addresses at example.com, example.net, example.org, or any other "example" domain ending with a three-letter top-level domain name. • For `regexp`: Enter regular expression. **Tip:** To validate syntax and correct matching, you can use the validator in the FortiMail GUI. For details, see the FortiMail Administration Guide. This setting is only available if sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `default` or `regexp`.	*
sender-pattern-group <group_name>	Enter the group of recipient email addresses. This setting is available only if sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `group`.	
sender-pattern-ldap-groupname <group_name>	Enter the group of recipient email addresses that is in the directory server. This setting is available only if sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `ldap`. **Note**: Use `$s` in the LDAP query string to match sender email addresses.	
sender-pattern-ldap-profile <profile_name>	Enter an LDAP profile. This setting is available only if sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp} is `ldap`.	
sender-pattern-type {default | external | group | internal | ldap | ldap-query | regexp}	Select how you will define the sender email addresses that match the policy, either: • `default`: An email address or wild card pattern that can match multiple email addresses. Also configure sender-pattern <sender_pattern>. • `external`: Email addresses that are **not** at a protected domain. • `group`: A group of email addresses configured on the FortiMail unit. Also configure sender-pattern-group <group_name>. • `internal`: Email addresses that are at a protected domain. • `ldap`: A group of email addresses configured on a directory server such as Microsoft Active Directory. Also configure sender-pattern-ldap-profile	default

Variable	Description	Default
	<profile_name> and sender-pattern-ldap-groupname <group_name>. • `ldap-query`: An LDAP query to a directory server such as Microsoft Active Directory. Also configure sender-pattern-ldap-profile <profile_name>. **Note**: Use `$s` in the query string to match sender addresses. For example, to reject senders that are not in the recipient's allowed sender list: **a.** Create an ACL policy and in sender-pattern-type {default \| external \| group \| internal \| ldap \| ldap-query \| regexp}, select `ldap-query`. **b.** Select an LDAP profile where this user query string is used: `&(mail=$m)(!(allowedSenders=$s)))` **c.** In action {discard \| receive \| reject \| relay \| safe \| safe-relay}, select `reject`. For each recipient (`$m`), this will match a sender (`$s`) that is not (`!`) in their `allowedSenders` list, and the action will reject it. • `regexp`: A regular expression. Also configure sender-pattern <sender_pattern>. **Tip:** To validate syntax and correct matching, you can use the validator in the FortiMail GUI. For details, see the FortiMail Administration Guide.	
status {enable | disable}	Enable or disable the policy.	enable
tls-profile <profile_name>	If you want to allow or reject the connection based on whether the session attributes matches TLS profile, then select the TLS profile. • **Match:** Perform the selection in action {discard | receive | reject | relay | safe | safe-relay}. • **No Match:** Perform the selection in action {fail | tempfail} in the TLS profile.	

Related topics

profile geoip-group
profile session
policy access-control delivery
policy delivery-control
policy ip

profile antispam

Use this command to configure system-wide (or, if these commands are run from inside `config domain`, domain-specific) antispam profiles.

FortiMail can use many methods to detect spam, such as the FortiGuard Antispam service, DNSBL queries, Bayesian scanning, and heuristic scanning. Antispam profiles contain settings for these features that you may want to vary by policy. Depending on the feature, before you configure antispam policies, you may need to enable the feature or configure its system-wide settings.

Syntax

```
config profile antispam
   edit <profile_name>
      [set comment "<comment_str>"]
      set action-default <action-profile_name>
      set apply-action-default {enable | disable}
      set scan-max-size <bytes_int>
      set scan-bypass-on-auth {enable | disable}
      set scan-pdf {enable | disable}

      set fortiguard-antispam {enable | disable}
      set action-fortiguard <action-profile_name>
      set fortiguard-check-ip {enable | disable}
      set action-fortiguard-blockip <action-profile-name>
      set ip-reputation-level1-status {enable | disable}
      set ip-reputation-level2-status {enable | disable}
      set ip-reputation-level3-status {enable | disable}
      set action-ip-reputation-level1 <action-profile_name>
      set action-ip-reputation-level2 <action-profile_name>
      set action-ip-reputation-level3 <action-profile_name>
      set ip-threat-feed-status {enable | disable}
      set ip-threat-feed <feed_name>
      set action-ip-threat-feed <action-profile_name>
      set url-filter-status {enable | disable}
      set url-filter <filter_name>
      set url-filter-secondary <filter_name>
      set url-filter-secondary-status {enable | disable}
      set action-url-filter <action-profile_name>
      set action-url-filter-secondary <action-profile_name>
      set spam-outbreak-protection {enable | disable | monitor-only}

      set greylist {enable | disable}
      set action-grey-list <action-profile_name>

      set spf-checking {enable | disable}
      set spf-fail-status {enable | disable}
      set spf-neutral-status {enable | disable}
      set spf-none-status {enable | disable}
      set spf-pass-status {enable | disable}
      set spf-perm-error-status {enable | disable}
      set spf-soft-fail-status {enable | disable}
```

```
set spf-temp-error-status {enable | disable}
set action-spf-fail <action-profile_name>
set action-spf-neutral <action-profile_name>
set action-spf-none <action-profile_name>
set action-spf-pass <action-profile_name>
set action-spf-perm-error <action-profile_name>
set action-spf-soft-fail <action-profile_name>
set action-spf-temp-error <action-profile_name>

set dkim-checking {enable | disable}
set dkim-fail-status {enable | disable}
set dkim-none-status {enable | disable}
set dkim-pass-status {enable | disable}
set dkim-temp-error-status {enable | disable}
set action-dkim-fail <action-profile_name>
set action-dkim-none <action-profile_name>
set action-dkim-pass <action-profile_name>
set action-dkim-temp-error <action-profile_name>

set dmarc-checking {enable | disable}
set dmarc-fail-status {enable | disable}
set dmarc-none-status {enable | disable}
set dmarc-pass-status {enable | disable}
set dmarc-temp-error-status {enable | disable}
set dmarc-override-option {override-dkim override-spf}
set action-dmarc-fail <action-profile_name>
set action-dmarc-none <action-profile_name>
set action-dmarc-pass <action-profile_name>
set action-dmarc-temp-error <action-profile_name>

set arc-status {enable | disable}
set arc-override-option {override-dkim override-dmarc override-spf}
set action-arc <action-profile_name>

set behavior-analysis {enable | disable}
set action-behavior-analysis <action-profile_name>

set bec-scan-status {enable | disable}
set weighted-analysis-status {enable | disable}
set weighted-analysis-profile <profile_name>
set action-weighted-analysis <action-profile-name>
set impersonation-analysis {enable | disable}
set impersonation <profile_name>
set action-impersonation-analysis <action-profile_name>
set cousin-domain {enable | disable}
set cousin-domain-profile <cousin-profile_name>
set cousin-domain-scan-option {auto-detection body-detection header-detection}
set action-cousin-domain <action-profile_name>
set sender-alignment-status {enable | disable}
set sender-alignment-option {display-name reply-to}
set action-sender-alignment <action-profile_name>

set heuristic {enable | disable}
set heuristic-rules-percent <percentage_int>
set heuristic-lower <threshold_float>
set heuristic-upper {threshold_float}
set action-heuristic <action-profile_name>
```

```
        set surbl {enable | disable}
        config surbl-server
           edit <surbl_name>
        end
        set action-surbl <action-profile_name>

        set dnsbl {enable | disable}
        config dnsbl-server
           edit <dnsbl_name>
        end
        set action-rbl <action-profile_name>

        set deepheader-analysis {enable | disable}
        set deepheader-check-ip {enable | disable}
        set action-deep-header <action-profile_name>

        set banned-word {enable | disable}
        config bannedwords
           edit <word_str>
              set subject {enable | disable}
              set body {enable | disable}
           next
        end
        set action-banned-word <action-profile_name>

        set safelist-word {enable | disable}
        config safelistwords
           edit <word_str>
              set subject {enable | disable}
              set body {enable | disable}
           next
        end

        set dictionary {enable | disable}
        set dictionary-type {group | profile}
        set dictionary-profile <profile_name>
        set dictionary-group <group-name>
        set dict-score <threshold_int>
        set action-dictionary <action-profile_name>

        set image-spam {enable | disable}
        set aggressive {enable | disable}
        set action-image-spam <action-profile_name>

        set bayesian {enable | disable}
        set bayesian-usertraining {enable | disable}
        set bayesian-autotraining {enable | disable}
        set bayesian-user-db {enable | disable}
        set action-bayesian <action-profile_name>

        set suspicious-newsletter-status {enable | disable}
        set action-suspicious-newsletter <action-profile_name>

        set newsletter-status {enable | disable}
        set action-newsletter <action-profile_name>
end
```

Variable	Description	Default
<dnsbl_name>	Enter a DNSBL server name to perform a DNSBL scan. The FortiMail unit will query DNS blocklist servers.	
<profile_name>	Enter the name of the profile.	
<surbl_name>	Enter a SURBL server name to perform a SURBL scan. The FortiMail unit will query SURBL servers.	
<word_str>	Enter the word to scan for. You can use wildcards to match multiple words. Regular expressions are not supported. For more information about wildcards and regular expressions, see the FortiMail Administration Guide.	
action-arc <action-profile_name>	Enter the action profile that FortiMail uses if the ARC scan determines that the email is spam.	
action-banned-word <action-profile_name>	Enter the action profile that FortiMail uses if the banned word scan determines that the email is spam.	
action-bayesian <action-profile_name>	Enter the action profile that FortiMail uses if the Bayesian scan determines that the email is spam.	
action-behavior-analysis <action-profile_name>	Enter the action profile that FortiMail uses if the behavior analysis scan determines that the email is spam.	
action-cousin-domain <action-profile_name>	Enter the action profile that FortiMail uses if the cousin domain scan determines that the email is spam.	
action-deep-header <action-profile_name>	Enter the action profile that FortiMail uses if the deep header scan determines that the email is spam.	
action-default <action-profile_name>	Enter the default action profile for scans. If you want a scan to use a different action profile, select it for that specific scan instead of accepting the default.	
action-dictionary <action-profile_name>	Enter the action profile that FortiMail uses if the heuristic scan determines that the email is spam.	
action-dkim-fail <action-profile_name>	Enter the action profile that FortiMail uses if an email does not pass the DKIM scan.	
action-dkim-none <action-profile_name>	Enter the action profile that FortiMail uses if no DKIM DNS record is not found or parsed correctly.	
action-dkim-pass <action-profile_name>	Enter the action profile that FortiMail uses if an email passes the DKIM scan.	

Variable	Description	Default
action-dkim-temp-error <action-profile_name>	Enter the action profile that FortiMail uses if the DNS server returns a temporary error when querying the DKIM record.	
action-dmarc-fail <action-profile_name>	Enter the action profile that FortiMail uses if an email does not pass the DMARC scan.	
action-dmarc-none <action-profile_name>	Enter the action profile that FortiMail uses if no DMARC DNS record is not found or parsed correctly.	
action-dmarc-pass <action-profile_name>	Enter the action profile that FortiMail uses if an email passes the DMARC scan.	
action-dmarc-policy-reject <action-profile_name>	Enter the action profile that FortiMail uses if an email matches a `reject` DMARC policy in the DNS records.	
action-dmarc-temp-error <action-profile_name>	Enter the action profile that FortiMail uses if DNS server returns Temp error when querying the DMARC DNS record.	
action-fortiguard-blockip <action-profile-name>	Enter the action profile that FortiMail uses if the FortiGuard block IP scan determines that the email is spam.	
action-fortiguard <action-profile_name>	Enter the action profile that FortiMail uses if the FortiGuard Antispam scan determines that the email is spam.	
action-grey-list <action-profile_name>	Enter the action profile that FortiMail uses if the greylist scan determines that the email is spam.	
action-heuristic <action-profile_name>	Enter the action profile that FortiMail uses if the heuristic scan determines that the email is spam.	
action-image-spam <action-profile_name>	Enter the action profile that FortiMail uses if the image scan determines that the email is spam.	
action-impersonation-analysis <action-profile_name>	Enter the action profile that FortiMail uses if impersonation analysis determines that the email is from someone impersonating a known email address.	
action-ip-reputation-level1 <action-profile_name>	Enter the action profile that FortiMail uses if the IP reputation scan results is level 1.	
action-ip-reputation-level2 <action-profile_name>	Enter the action profile that FortiMail uses if the IP reputation scan result is level 2.	
action-ip-reputation-level3 <action-profile_name>	Enter the action profile that FortiMail uses if the IP reputation scan result is level 3.	

Variable	Description	Default
action-ip-threat-feed <action-profile_name>	Enter the action profile that FortiMail uses if the threat feed scan determines that the email is spam.	
action-newsletter <action-profile_name>	Enter the action profile that FortiMail uses if the newsletter scan determines that the email is spam.	
action-rbl <action-profile_name>	Enter the action profile that FortiMail uses if the DNSBL scan determines that the email is spam.	
action-sender-alignment <action-profile_name>	Enter the action profile that FortiMail uses if the email does not pass the sender alignment scan.	
action-spf-fail <action-profile_name>	Enter the action profile that FortiMail uses if the email does not pass the SPF scan, which means the host is not authorized to send messages.	
action-spf-neutral <action-profile_name>	Enter the action profile that FortiMail uses if the SPF scan result is neutral, which means the SPF record is found but no definitive assertion.	
action-spf-none <action-profile_name>	Enter the action profile that FortiMail uses if the SPF scan has no result, which means there is no SPF record.	
action-spf-pass <action-profile_name>	Enter the action profile that FortiMail uses if email passes the SPF scan, which means the host is authorized to send a message.	
action-spf-perm-error <action-profile_name>	Enter the action profile that FortiMail uses if the SPF scan has a permanent error, which means the SPF records are invalid.	
action-spf-soft-fail <action-profile_name>	Enter the action profile that FortiMail uses if the SPF scan has a soft failure, which means the host is not authorized to send messages, but it's not a strong statement.	
action-spf-temp-error <action-profile_name>	Enter the action profile that FortiMail uses if the SPF scan has a temporary error, which means there is a processing error.	
action-surbl <action-profile_name>	Enter the action profile that FortiMail uses if the SURBL scan determines that the email is spam.	
action-suspicious-newsletter <action-profile_name>	Enter the action profile that FortiMail uses if the suspicious newsletter scan determines that the email is spam.	
action-url-filter-secondary <action-profile_name>	Enter the action profile that FortiMail uses if the URL filter scan determines that the email is spam.	
action-url-filter <action-profile_name>	Enter the action profile that FortiMail uses if the URL filter scan determines that the email is spam.	

Variable	Description	Default
action-weighted-analysis <action-profile-name>	Enter the action profile that FortiMail uses if weighted analysis determines that the email is spam.	
aggressive {enable | disable}	Enable this option to examine file attachments in addition to images embedded in the message body. **Tip:** To improve performance, enable this option only if you do not have a satisfactory spam detection rate.	disable
apply-action-default {enable | disable}	Enable to perform the action in `action-default <action-profile_name>` immediately, without applying other antispam filters, if the email matches the IP or recipient policy	disable
arc-override-option {override-dkim override-dmarc override-spf}	Select whether the ARC result has priority over SPF, DKIM, and/or DMARC. This can be useful when a policy matches indirectly delivered email (via mailing list, forwarding service, etc.) that, during normal processing, always invalidates SPF or DKIM signatures. The override allows FortiMail to validate the email using the alternative ARC signature instead.	
arc-status {enable | disable}	Enable Authenticated Received Chain (ARC) validation to detect if the email was modified in transit by a relay or proxy. Also configure `arc-sealing-option {all | disable | incoming | outgoing}`.	disable
banned-word {enable | disable}	Enable to perform a banned words scan.	disable
bayesian-autotraining {enable | disable}	Enable to use FortiGuard Antispam and SURBL scan results to train per-user Bayesian databases that are not yet mature (that is, they have not yet been trained with 200 legitimate email and 100 spam in order to recognize spam).	enable
bayesian-user-db {enable | disable}	Enable to use per-user Bayesian databases. If disabled, the Bayesian scan will use either the global or the per-domain Bayesian database, whichever is selected for the protected domain.	disable
bayesian-usertraining {enable | disable}	Enable to accept email forwarded from email users to the Bayesian control email addresses in order to train the Bayesian databases to recognize spam and legitimate email.	enable

Variable	Description	Default
bayesian {enable | disable}	Enable to perform a Bayesian scan.	disable
bec-scan-status {enable | disable}	Enable to perform a business email compromise (BEC) scan. Then configure which scans in `cousin-domain {enable | disable}`, `impersonation-analysis {enable | disable}`, `sender-alignment-status {enable | disable}`, and `weighted-analysis-status {enable | disable}`.	disable
behavior-analysis {enable | disable}	Enable to analyze the similarities between uncertain email and known email in the behavior analysis (BA) database to determine whether the uncertain email is spam. To adjust the aggressiveness of the scan, see also antispam behavior-analysis on page 42	disable
body {enable | disable}	Enable to scan the email message bodies for the word.	disable
comment "<comment_str>"	Enter a description or comment.	
cousin-domain-profile <cousin-profile_name>	Select which cousin domain profile to use. This setting takes effect if `cousin-domain {enable | disable}` is `enable`.	
cousin-domain-scan-option {auto-detection body-detection header-detection}	Select where in the email to scan for domain name impersonation, either automatically, within the email body, and/or the message headers. This setting takes effect if `cousin-domain {enable | disable}` is `enable`.	header-detection body-detection auto-detection
cousin-domain {enable | disable}	Enable to perform a cousin domain (domain impersonation) scan. This detects domain names that are deliberately misspelled in order to appear to come from a trusted domain. Then also configure `cousin-domain-profile <cousin-profile_name>`, `cousin-domain-scan-option {auto-detection body-detection header-detection}`, and `action-cousin-domain <action-profile_name>`. This setting takes effect if `bec-scan-status {enable | disable}` is `enable`.	disable
deepheader-analysis {enable | disable}	Enable to inspect all message headers for known spam characteristics. If the FortiGuard Antispam scan is enabled, this option uses results from that scan, providing up-to-date header analysis.	disable

Variable	Description	Default
deepheader-check-ip {enable | disable}	Enable to query for the blocklist status of the IP addresses of all SMTP servers appearing in the `Received:` message header. If this option is disabled, the FortiMail unit examines only the IP address of the current SMTP client. This option requires that you also configure either or both FortiGuard Antispam scan and DNSBL scan.	disable
dict-score <threshold_int>	Enter the threshold for dictionary profile matches. When the dictionary profile scans an email, it counts the number of matching words or phrases, and adjusts this total according to `pattern-weight <weight_int>` and `pattern-max-weight <weight_int>`. If the result equals or exceeds this threshold, then FortiMail applies the action in `action-dictionary <action-profile_name>`.	
dictionary-group <group-name>	Select which dictionary profile group to use. This setting is available if `dictionary-type {group | profile}` is `group`.	
dictionary-profile <profile_name>	Select which dictionary profile to use. This setting is available if `dictionary-type {group | profile}` is `profile`.	
dictionary-type {group | profile}	Select whether to use a single dictionary profile, or a group of dictionary profiles. Then also configure `dictionary-profile <profile_name>` or `dictionary-group <group-name>`.	profile
dictionary {enable | disable}	Enable to perform a dictionary scan. Also configure `dictionary-type {group | profile}` and `dict-score <threshold_int>`.	disable
dkim-checking {enable | disable}	Enable to perform a DKIM scan. Also configure related options for each possible DKIM result, such as `dkim-fail-status {enable | disable}` with `action-dkim-fail <action-profile_name>`. Also configure `dkim-signing-option {all | disable | incoming | outgoing}`. If either SPF or DKIM scans pass, then the DMARC scan will pass. If both fail, then DMARC fails.	disable
dkim-fail-status {enable | disable}	Enable or disable checking invalid DKIM body hash or signature.	enable

Variable	Description	Default
dkim-none-status {enable | disable}	Enable or disable checking for instances where the DNS server has no DKIM record, or the record could not be correctly parsed.	disable
dkim-pass-status {enable | disable}	Enable or disable DKIM check passing.	disable
dkim-temp-error-status {enable | disable}	Enable or disable checking for instances where DNS server returns a temporary error when querying the DKIM DNS record.	disable
dmarc-checking {enable | disable}	Enable to have the unit perform email authentication with SPF and DKIM checking. If either SPF check or DKIM check passes, DMARC check will pass. If both fail, DMARC fails.	enable
dmarc-fail-status {enable | disable}	Enable or disable DMARC check failing.	enable
dmarc-none-status {enable | disable}	Enable or disable checking for instances where no DMARC DNS record is found, or the record could not be correctly parsed.	disable
dmarc-override-option {override-dkim override-spf}	Select if you want the DMARC result to take precedence over SPF and/or DKIM results. For example, if DMARC verification succeeds, then the SPF fail and soft fail won't take effect anymore.	
dmarc-pass-status {enable | disable}	Enable or disable performing an action when the DMARC check result is a pass. Also configure `action-dmarc-pass <action-profile_name>`.	disable
dmarc-temp-error-status {enable | disable}	Enable or disable checking for instances where DNS server returns Temp error when querying the DMARC DNS record. Also configure `action-dmarc-temp-error <action-profile_name>`.	disable
dnsbl {enable | disable}	Enable to perform a DNSBL scan. The FortiMail unit will query DNS blocklist servers defined using `<dnsbl_name>`.	disable
fortiguard-antispam {enable | disable}	Enable for the FortiMail unit to query the FortiGuard Antispam service to determine if any of the uniform resource locators (URL) in the message body are associated with spam. If any URL is blocklisted, the FortiMail unit considers the email to be spam, and you can select the action that the FortiMail unit will perform.	disable
fortiguard-check-ip {enable | disable}	Enable to perform a scan for whether or not the IP address of the SMTP client is blocklisted in the FortiGuard Antispam query.	disable

Variable	Description	Default
greylist {enable | disable}	Enable to perform a greylist scan.	disable
heuristic {enable | disable}	Enable to perform a heuristic scan.	disable
heuristic-lower <threshold_float>	Enter the score equal to or below which the FortiMail unit considers an email to **not** be spam.	-20.000000
heuristic-rules-percent <percentage_int>	Enter the percentage of the total number of heuristic rules that will be used to calculate the heuristic score for an email message. The FortiMail unit compares this total score to the upper and lower level threshold to determine if an email is: • spam • not spam • indeterminable (score is between the upper and lower level thresholds) To improve system performance and resource efficiency, enter the lowest percentage of heuristic rules that results in a satisfactory spam detection rate.	25
heuristic-upper {threshold_float}	Enter the score equal to or above which the FortiMail unit considers an email to be spam.	3.500000
image-spam {enable | disable}	Enable to perform an image spam scan.	disable
impersonation-analysis {enable | disable}	Enable to perform a sender impersonation analysis scan. This automatically learns and tracks the mapping of display names and internal email addresses to prevent spoofing attacks. Then also configure `impersonation <profile_name>` and `action-impersonation-analysis <action-profile_name>`. This setting takes effect if `bec-scan-status {enable | disable}` is `enable`.	disable
impersonation <profile_name>	Enter the impersonation profile that FortiMail uses to prevent email spoofing attacks. This setting takes effect if `impersonation-analysis {enable | disable}` is `enable`.	disable
ip-reputation-level3-status {enable | disable}	Enable to query the FortiGuard Antispam service about the reputation of the public IP address of the SMTP client to determine if it is blocklisted.	disable
ip-reputation-level2-status {enable | disable}	Enable to query the FortiGuard Antispam service about the reputation of the public IP address of the SMTP client to determine if it is blocklisted.	disable

Variable	Description	Default
ip-reputation-level1-status {enable | disable}	Enable to query the FortiGuard Antispam service about the reputation of the public IP address of the SMTP client to determine if it is blocklisted. FortiGuard categorizes blocklisted IP addresses into three levels. Level 1 has the worst reputation and level 3 the best.	disable
ip-threat-feed-status {enable | disable}	Enable to detect spam by querying a threat feed. Also configure `ip-threat-feed <feed_name>`.	disable
ip-threat-feed <feed_name>	Enter the name of a threat feed profile.	
newsletter-status {enable | disable}	Enable to detect newsletters and other marketing campaigns that are not spam.	
safelist-enable {enable | disable}	Enable to automatically update personal safelist database from sent email.	disable
safelist-word {enable | disable}	Enable to perform a safelist word scan. Also configure `<word_str>`, `body {enable | disable}`, and `subject {enable | disable}`.	disable
scan-bypass-on-auth {enable | disable}	Enable to omit antispam scans when an SMTP sender is authenticated.	disable

scan-max-size <bytes_int>	Enter the maximum size, in bytes, that the FortiMail unit will scan for spam. Messages exceeding the limit will not be scanned for spam.
	To scan all email regardless of size, enter `0`.
		`1204`
		(for predefined profiles)
		
		`600`
		(for user-defined profiles)

scan-pdf {enable | disable}	Enable to scan the first page of PDF attachments using heuristic, banned word, and image spam scans, if they are enabled.	disable
sender-alignment-option {display-name reply-to}	Select which message headers (`From:` or `Reply-To:`) to compare with the SMTP envelope for the sender alignment check. This setting takes effect if sender-alignment-status {enable | disable} is `enable`.	
sender-alignment-status {enable | disable}	Enable to scan for sender email address and name mismatches. Sender alignment compares the message headers that you select in `sender-alignment-option {display-name reply-to}` with the SMTP envelope (`MAIL FROM:` to look for a mismatch, which is typical of spam. If the sender email address fails the check, FortiMail takes the action in `action-sender-alignment <action-profile_name>`.	disable

Variable	Description	Default
	This setting takes effect if `bec-scan-status {enable | disable}` is `enable`.	
spam-outbreak-protection {enable | disable | monitor-only}	Enable to temporarily hold suspicious email for a certain period of time (outbreak-protection-period <minutes_int>) if the enabled FortiGuard Antispam check (block IP and/or URL filter) returns no result. After the specified time interval, FortiMail will query the FortiGuard server again. This provides an opportunity for the FortiGuard Antispam service to update its database when a spam outbreak occurs. When set to `monitor-only`, email is **not** deferred. Instead, FortiMail inserts the message header `X-FEAS-Spam-outbreak: monitor-only`, and the email is logged.	disable
spf-checking {enable | disable}	Enable to have the FortiMail unit perform the action configured in this antispam profile, instead of the action configured in the session profile. See `spf-validation {enable | disable}` on page 259. You can specify different actions toward different SPF check results: • `spf-fail-status`:Host is not authorized to send messages. • `spf-soft-fail-status`: Host is not authorized to send messages but not a strong statement. • `spf-sender-alighnment-status`: Domain name in the message header `From:` and SMTP `AUTH` command do not match. • `spf-perm-error-status`: SPF records are invalid. • `spf-temp-error-status`: Temporary processing error. • `spf-pass-status`: Host is authorized to send messages. • `spf-neutral-status`: SPF record is found but no definitive assertion. • `spf-none-status`: No SPF record.	disable
spf-fail-status {enable | disable}	Enable to make the FortiMail unit check if the host is not authorized to send messages. If the client IP address fails the SPF check, FortiMail takes the antispam action entered in action-spf-fail.	
spf-neutral-status {enable | disable}	Enable to make the FortiMail unit check if the SPF record is found but no definitive assertion.	

Variable	Description	Default
	If the client IP address fails the SPF check, FortiMail takes the antispam action entered in action-spf-neutral.	
spf-none-status {enable | disable}	Enable to make the FortiMail unit check if there is no SPF record. If the client IP address fails the SPF check, FortiMail takes the antispam action entered in action-spf-none.	
spf-pass-status {enable | disable}	Enable to make the FortiMail unit check if the host is authorized to send messages. If the client IP address fails the SPF check, FortiMail takes the antispam action configured in action-spf-pass.	
spf-perm-error-status {enable | disable}	Enable to make the FortiMail unit check if the SPF records are invalid. If the client IP address fails the SPF check, FortiMail takes the antispam action entered in action-spf-perm-error.	
spf-soft-fail-status {enable | disable}	Enable to make the FortiMail unit check if the host is not authorized to send messages but not a strong statement. If the client IP address fails the SPF check, FortiMail takes the antispam action entered in action-spf-soft-fail.	enable
spf-temp-error-status {enable | disable}	Enable to make the FortiMail unit check if there is a processing error. If the client IP address fails the SPF check, FortiMail takes the antispam action entered in `action-spf-temp-error`.	
subject {enable | disable}	Enable to scan subject lines for the word.	disable
surbl {enable | disable}	Enable to perform a SURBL scan. The FortiMail unit will query SURBL servers defined using `<surbl_name>`.	disable
suspicious-newsletter-status {enable | disable}	Enable the detection of newsletters.	disable
url-filter-secondary-status {enable | disable}	Enable or disable the secondary URL filter scan.	disable

Variable	Description	Default
url-filter-secondary <filter_name>	To take different actions towards different URL filters/categories, you can specify a primary and a secondary filter, and specify different actions for each filter. If both URL filters match an email message, the primary filter action will take precedence.	
url-filter-status {enable | disable}	Enable or disable URL filter scan.	disable
url-filter <filter_name>	Enter the URL filter to use.	
weighted-analysis-profile <profile_name>	Enter the weighted analysis profile to use. This setting takes effect if `weighted-analysis-status {enable | disable}` is enable.	
weighted-analysis-status {enable | disable}	Enable or disable the weighted analysis profile scan. Then also configure `weighted-analysis-profile <profile_name>` and `action-weighted-analysis <action-profile-name>`. This setting takes effect if `bec-scan-status {enable | disable}` is enable.	disable

Related topics

- antispam settings
- domain
- profile antispam-action
- profile cousin-domain
- profile dictionary
- profile weighted-analysis
- system fortiguard antispam

profile antispam-action

Use this command to configure antispam action profiles.

Syntax

```
config profile antispam-action
```

```
    edit <profile_name>
       set action {discard | domain-quarantine | none | personal-quarantine | reject | rewrite-
            rcpt | system-quarantine}
       set alternate-host {<relay_fqdn> | <relay_ipv4>}
       set alternate-host-status {enable | disable}
       set archive-account <account_name>
       set archive-status {enable | disable}
       set bcc-addr <recipient_email>
       set bcc-env-from-addr <message_str>
       set bcc-env-from-status {enable |  disable}
       set bcc-status {enable | disable}
       set defer-delivery {enable | disable}
       set deliver-to-original-host {enable | disable}
       set disclaimer-insertion {enable | disable}
       set disclaimer-insertion-content <message_name>
       set disclaimer-insertion-location {beginning | end}
       set fortiguard-antispam-outbreak {enable | disable}
       set header-insertion-name <name_str>
       set header-insertion-status {enable | disable}
       set header-insertion-value <header_str>
       set notification-profile <profile_name>
       set notification-status {enable | disable}
       set quarantine-notify {enable | disable}
       set quarantine-notify-profile <profile_name>
       set rewrite-rcpt-local-type {none | prefix | replace | suffix}
       set rewrite-rcpt-local-value <value_str>
       set rewrite-rcpt-domain-type {none-prefix | replace | suffix}
       set rewrite-rcpt-domain-value <value_str>
end
```

Variable	Description	Default
<profile_name>	Enter the name of an antispam action profile.	
action {discard | domain-quarantine | none | personal-quarantine | reject | rewrite-rcpt | system-quarantine}	Enter an action for the profile. • `discard`: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. • `domain-quarantine`: Enter to redirect spam to the per-domain quarantine. For more information, see the FortiMail Administration Guide. Note that this option is only available with a valid advanced management license. • `none`: Apply any configured header or subject line tags, if any. • `personal-quarantine`: Enter to redirect spam to the per-recipient quarantine. For more information, see the FortiMail Administration Guide. This option is available only for incoming profiles. • `reject`: Enter to reject the email and reply to the SMTP client with SMTP reply code 550. • `rewrite-rcpt`: Enter to change the recipient address of any email message detected as spam. Configure rewrites separately for the local-part (the portion of the email address before the '@' symbol, typically a user name) and the domain part (the portion of the email address after the '@' symbol).	none

Variable	Description	Default
	If you enter this option, also configure rewrite-rcpt-local-type {none | prefix | replace | suffix}, rewrite-rcpt-local-value <value_str>, rewrite-rcpt-domain-type {none-prefix | replace | suffix}, and rewrite-rcpt-domain-value <value_str>. • `system-quarantine`: Enter to redirect spam to the system quarantine. For more information, see the FortiMail Administration Guide.	
alternate-host {<relay_fqdn> | <relay_ipv4>}	Type the fully qualified domain name (FQDN) or IP address of the alternate relay or SMTP server. This field applies only if `alternate-host-status` is `enable`.	
alternate-host-status {enable | disable}	Enable to route the email to a specific SMTP server or relay. Also configure alternate-host {<relay_fqdn> | <relay_ipv4>}. **Note**: If you enable this setting, for all email that matches the profile, the FortiMail unit will use this destination and ignore mailsetting relay-host-list and the protected domain's tp-use-domain-mta {yes | no}.	disable
archive-account <account_name>	Type the email archive account name where you want to archive the spam. For more information about archive accounts, see archive policy on page 65.	
archive-status {enable | disable}	Enable to allow the archive-account <account_name> function to work.	disable
bcc-addr <recipient_email>	Type the blind carbon copy (BCC) recipient email address. This field applies only if `bcc-status` is `enable`.	
bcc-env-from-addr <message_str>	Specify an envelope from BCC address. In the case that email is not deliverable and bounced back, the email is returned to the specified envelope from address instead of the original sender. This is helpful when you want to use a specific email to collect bounce notifications. This field applies only if `bcc-env-from-status` is `enable`.	
bcc-env-from-status {enable | disable}	Enable to specify an envelope from address.	disable
bcc-status {enable | disable}	Enable to send a BCC of the email. Also configure bcc-addr <recipient_email>.	disable
defer-delivery {enable | disable}	Enable to defer delivery of emails that may be resource intensive and reduce performance of the mail server, such as large email messages, or lower priority email from certain senders (for example, marketing campaign email and mass mailing).	disable
deliver-to-original-host {enable | disable}	Enable to deliver the message to the original host.	disable
disclaimer-insertion {enable | disable}	Enable to insert a disclaimer. See also disclaimer-insertion {selected-message | all-message}.	disable

Variable	Description	Default
disclaimer-insertion-content <message_name>	Enter the name of the disclaimer to insert.	default
disclaimer-insertion-location {beginning | end}	Select whether to insert the disclaimer at the start or end of the email.	beginning
fortiguard-antispam-outbreak {enable | disable}	Enable to manually defer emails and place email in the spam defer queue. **Note:** The *Spam outbreak protection* option under *System > FortiGuard > AntiSpam* does not affect this feature.	disable
header-insertion-name <name_str>	Enter the message header key. The FortiMail unit will add this text to the message header of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes, including a spam mailbox, based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client. Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Custom-Header: Detected as spam by profile 22.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key. **Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822. See header-insertion-value <header_str>.	
header-insertion-status {enable | disable}	Enable to add a message header to detected spam. See header-insertion-value <header_str>.	disable
header-insertion-value <header_str>	Enter the message header value. Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Custom-Header: Detected as spam by profile 22.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key. **Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822. See header-insertion-name <name_str>.	
notification-profile <profile_name>	Type the name of the notification profile used for sending notifications.	
notification-status {enable | disable}	Enable sending notifications using a notification profile.	disable

Variable	Description	Default
quarantine-notify {enable | disable}	Enable to quarantine and also notify the recipient about the action.	disable
quarantine-notify-profile <profile_name>	Enter the name of a notification profile.	
rewrite-rcpt-local-type {none | prefix | replace | suffix}	Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any email message detected as spam. `none`: No change. `prefix`: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str>. `suffix`: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>. `replace`: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str>.	none
rewrite-rcpt-local-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-local-type {none | prefix | replace | suffix}.	
rewrite-rcpt-domain-type {none-prefix | replace | suffix}	Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any email message detected as spam. `none`: No change. `prefix`: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. `suffix`: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. `replace`: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <value_str>.	none
rewrite-rcpt-domain-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-domain-type {none-prefix | replace | suffix}.	

Related topics

profile antispam
mailsetting preference

profile antivirus

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

The FortiMail unit scans email header, body, and attachments (including compressed files, such as ZIP, PKZIP, LHA, ARJ, and RAR files) for virus infections. If the FortiMail unit detects a virus, it will take actions as you define in the antivirus action profiles.

Syntax

```
config profile antivirus
   edit <profile_name>
      set action-default { predefined_av_discard | predefined_av_reject}
      set action-file-signature
      set action-heuristic {predefined_av_discard |  predefined_av_reject}
      set action-outbreak <action>
      set action-sandbox-high <action>
      set action-sandbox-low <action>
      set action-sandbox-medium <action>
      set action-sandbox-noresult <action>
      set action-sandbox-url-high <action>
      set action-sandbox-url-low <action>
      set action-sandbox-url-medium <action>
      set action-sandbox-url-noresult <action>
      set action-sandbox-url-virus <action>
      set action-sandbox-virus <action>
      set file-signature-check {enable | disable}
      set grayware-scan {enable | disable}
      set heuristic {enable | disable}
      set malware-outbreak-protection {enable | disable}
      set sandbox-analysis {enable | disable}
      set sandbox-analysis-url{enable | disable}
      set sandbox-scan-mode {submit-and-wait | submit-only}
      set scanner {enable | disable}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	
action-default { predefined_av_discard | predefined_av_reject}	Type a predefined antivirus action. `predefined_av_discard`: Accept infected email, but then delete it instead of delivering the email, without notifying the SMTP client. `predefined_av_reject`: Reject infected email and reply to the SMTP client with SMTP reply code 550.	

action-file-signature	Type a predefined scan for the file signature action.
	`predefined_av_discard:`
	`predefined_av_reject:`	

action-heuristic {predefined_av_discard | predefined_av_reject}	Type a predefined heuristic scanning action on infected email. `predefined_av_discard`: Accept email suspected to be infected, but then delete it instead of delivering the email, without notifying the SMTP client. `predefined_av_reject`: Reject email suspected to be infected, and reply to the SMTP client with SMTP reply code 550.	

Variable	Description	Default
action-outbreak <action>	Type to determine the action to take if the FortiSandbox analysis determines that the email message has an outbreak.	
action-sandbox-high <action>	Type to determine the action to take if the FortiSandbox attachment analysis determines that the email messages have high probability of viruses or other threat qualities.	default
action-sandbox-low <action>	Type to determine the action to take if the FortiSandbox attachment analysis determines that the email messages have low probability of viruses or other threat qualities.	default
action-sandbox-medium <action>	Type to determine the action to take if the FortiSandbox attachment analysis determines that the email messages have medium probability of viruses or other threat qualities.	default
action-sandbox-virus <action>	Type to determine the action to take if the FortiSandbox attachment analysis determines that the email messages definitely have viruses or other threat qualities.	default
action-sandbox-noresult <action>	Type to determine the action to take if the FortiSandbox attachment analysis returns no results.	None
action-sandbox-url-high <action>	Type to determine the action to take if the FortiSandbox URL analysis determines that the email messages have high probability of viruses or other threat qualities.	default
action-sandbox-url-low <action>	Type to determine the action to take if the FortiSandbox URL analysis determines that the email messages have low probability of viruses or other threat qualities.	default
action-sandbox-url-medium <action>	Type to determine the action to take if the FortiSandbox URL determines that the email messages have medium probability of viruses or other threat qualities.	default
action-sandbox-url-virus <action>	Type to determine the action to take if the FortiSandbox URL analysis determines that the email messages definitely have viruses or other threat qualities.	default
action-sandbox-url-noresult <action>	Type to determine the action to take if the FortiSandbox URL analysis returns no results.	None
file-signature-check {enable | disable}	Enable to scan for file signatures.	disable
grayware-scan {enable | disable}	Enable to scan for grayware as well when performing antivirus scanning.	enable
heuristic {enable | disable}	Enable to use heuristics when performing antivirus scanning.	enable

Variable	Description	Default
malware-outbreak-protection {enable | disable}	Instead of using virus signatures, malware outbreak protection uses data analytics from the FortiGuard Service. For example, if a threshold volume of previously unknown attachments are being sent from known malicious sources, they are treated as suspicious viruses. This feature can help quickly identify new threats. Because the infected email is treated as virus, the virus replacement message will be used, if the replacement action is triggered.	
sandbox-analysis {enable | disable}	Enable to send suspicious email attachments to FortiSandbox for inspection. For details about FortiSandbox, see system fortisandbox on page 308.	disable
sandbox-analysis-url {enable | disable}	Enable or disable sending suspicious attachment content to FortiSandbox for analysis.	disable
sandbox-scan-mode {submit-and-wait | submit-only}	Select how the email is handled by the FortiSandbox.	submit-and-wait
scanner {enable | disable}	Enable to perform antivirus scanning for this profile.	disable

Related topics

file signature

profile antispam

profile antivirus-action

Use this command to configure antivirus action profiles.

Syntax

```
config profile antivirus-action
   edit <profile_name>
      config header-insertion-list
         edit <header-name>
            set header-insertion-value <string>
         next
      end
      set action {discard | domain-quarantine | none | reject | repackage | repackage-with-cmsg |
            rewrite-rcpt | system-quarantine}
      set alternate-host {<relay_fqdn> | <relay_ipv4>}
      set alternate-host-status {enable | disable}
```

```
        set archive-account
        set archive-status
        set bcc-addr <recipient_email>
        set bcc-env-from-addr <message_str>
        set bcc-env-from-status {enable | disable}
        set bcc-status {enable | disable}
        set deliver-to-original-host {enable | disable}
        set disclaimer-insertion {enable | disable}
        set disclaimer-insertion-content <message_name>
        set disclaimer-insertion-location {beginning | end}
        set header-insertion-name <name_str>
        set header-insertion-status {enable | disable}
        set header-insertion-value <header_str>
        set notification-profile <profile_name>
        set notification-status {enable | disable}
        set quarantine-notify {enable | disable}
        set quarantine-notify-profile <profile_name>
        set remove-url-status {enable | disable}
        set replace-infected-status {enable | disable}
        set rewrite-rcpt-local-type {none | prefix | replace | suffix}
        set rewrite-rcpt-local-value <value_str>
        set rewrite-rcpt-domain-type {none-prefix | replace | suffix}
        set rewrite-rcpt-domain-value <value_str>
        set subject-tagging-status {enable | disable}
        set subject-tagging-text <tag_str>
end
```

Variable	Description	Default
<profile_name>	Enter the name of an antivirus action profile.	
action {discard | domain-quarantine | none | reject | repackage | repackage-with-cmsg | rewrite-rcpt | system-quarantine}	Enter an action for the profile. • `discard`: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. • `domain-quarantine`: Enter to redirect virus to the per-domain quarantine. For more information, see the FortiMail Administration Guide. Note that this option is only available with a valid advanced management license. • `none`: Apply any configured header or subject line tags, if any. • `reject`: Enter to reject the email and reply to the SMTP client with SMTP reply code 550. • `repackage`: Forward the infected email as an attachment but the original email body will still be used without modification. • `repackage-with-cmsg`: Forward the infected email as an attachment with the customized email body that you define in the custom email template. For example, in the template, you may want to say “The attached email is infected by a virus”. • `rewrite-rcpt`: Enter to change the recipient address of any email message detecting a virus. Configure rewrites separately for the local-part (the portion of the email address before the "@" symbol, typically a user name) and the domain part (the portion of the email address after the "@" symbol). If you enter this option, also configure rewrite-rcpt-local-type	none

Variable	Description	Default
	{none | prefix | replace | suffix}, rewrite-rcpt-local-value <value_str>, rewrite-rcpt-domain-type {none-prefix | replace | suffix}, and rewrite-rcpt-domain-value <value_str>. • `system-quarantine`: Enter to redirect virus to the system quarantine. For more information, see the FortiMail Administration Guide.	
alternate-host {<relay_fqdn> | <relay_ipv4>}	Type the fully qualified domain name (FQDN) or IP address of the alternate relay or SMTP server. This field applies only if `alternate-host-status` is `enable`.	
alternate-host-status {enable | disable}	Enable to route the email to a specific SMTP server or relay. Also configure alternate-host {<relay_fqdn> | <relay_ipv4>}. **Note**: If you enable this setting, for all email that matches the profile, the FortiMail unit will use this destination and ignore mailsetting relay-host-list and the protected domain's tp-use-domain-mta {yes | no}.	disable
archive-account	Enter the archive account.	
archive-status	Enable or disable message archiving.	disable
bcc-addr <recipient_email>	Type the blind carbon copy (BCC) recipient email address. This field applies only if `bcc-status` is `enable`.	
bcc-env-from-addr <message_str>	Specify an envelope from BCC address. In the case that email is not deliverable and bounced back, the email is returned to the specified envelope from address instead of the original sender. This is helpful when you want to use a specific email to collect bounce notifications. This field applies only if `bcc-env-from-status` is `enable`.	
bcc-env-from-status {enable | disable}	Enable to specify an envelope from address.	disable
bcc-status {enable | disable}	Enable to send a BCC of the email. Also configure bcc-addr <recipient_email>.	disable
deliver-to-original-host {enable | disable}	Enable to deliver the message to the original host.	disable
disclaimer-insertion {enable | disable}	Enable to insert disclaimer.	disable
disclaimer-insertion-content <message_name>	Specify the content name to be inserted.	default
disclaimer-insertion-location {beginning | end}	Insert the disclaimer at the beginning or end.	beginning
header-insertion-name <name_str>	Enter the message header key. The FortiMail unit will add this text to the message header of the email before forwarding it to the recipient.	

Variable	Description	Default
	Many email clients can sort incoming email messages into separate mailboxes based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client. Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Custom-Header: Detected as virus by profile 22.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key. **Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822. See header-insertion-value <header_str>.	
header-insertion-status {enable | disable}	Enable to add a message header to detected virus. See header-insertion-value <header_str>.	disable
header-insertion-value <header_str>	Enter the message header value. Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Custom-Header: Detected as virus by profile 22.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key. **Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822. See header-insertion-name <name_str>.	
notification-profile <profile_name>	Type the name of the notification profile used for sending notifications.	
notification-status {enable | disable}	Enable sending notifications using a notification profile.	disable
quarantine-notify {enable | disable}	Enable to quarantine and also notify the recipient about the action.	disable
quarantine-notify-profile <profile_name>	Enter the name of a notification profile.	
remove-url-status {enable | disable}	Enable to remove URL detected by FortiSandbox.	enable
replace-infected-status {enable | disable}	Enable or disable the option to replace infected body or attachment.	disable

Variable	Description	Default
rewrite-rcpt-local-type {none | prefix | replace | suffix}	Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any email message detecting a virus. none: No change. prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str>. suffix: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>. replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str>.	none
rewrite-rcpt-local-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-local-type {none | prefix | replace | suffix}.	
rewrite-rcpt-domain-type {none-prefix | replace | suffix}	Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any email message detecting a virus. none: No change. prefix: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. suffix: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. replace: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <value_str>.	none
rewrite-rcpt-domain-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-domain-type {none-prefix | replace | suffix}.	
subject-tagging-status {enable | disable}	Enable to prepend text defined using subject-tagging-text <tag_str> (“tag") to the subject line on detected virus.	disable
subject-tagging-text <tag_str>	Enter the text that will appear in the subject line of the email, such as “[VIRUS] ". The FortiMail unit will prepend this text to the subject line of virus before forwarding it to the recipient.	

Related topics

profile antivirus

profile authentication

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

FortiMail units support the following authentication methods:

- IMAP
- POP3
- RADIUS
- SMTP

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

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

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

For more information, see the FortiMail Administration Guide.

Syntax

```
config profile authentication imap
   edit <profile_name>
      set auth-type {auto | cram-md5 | digest-md5 | login | ntlm | plain}
      set option {ssl secure tls senddomain}
      set port <port_int>
      set server {<fqdn_str> | <host_ipv4>}
config profile authentication pop3
   edit <profile_name>
      set auth-type {auto | cram-md5 | digest-md5 | login | ntlm | plain}
      set option {ssl secure tls senddomain}
      set port <port_int>
      set server {<fqdn_str> | <host_ipv4>}
config profile authentication radius
   edit <profile_name>
      set access-override {enable | disable}
      set access-override-attribute <integer>
      set  access-override-vendor <integer>
      set auth-prot {auto | chap | mschap | mschap2 | pap}
      set domain-override {enable | disable}
      set domain-override-attribute <integer>
      set domain-override-vendor <integer>
      set nas-ip <ip_addr>
      set port <port_int>
      set secret <password_str>
      set send-domain {enable | disable}
      set server {<fqdn_str> | <host_ipv4>}
config profile authentication smtp
   edit <profile_name>
      set auth-type {auto | cram-md5 | digest-md5 | login | ntlm | plain}
      set option {ssl secure tls senddomain}
      set server {<fqdn_str> | <host_ipv4>}
      set port <port_int>
      set try-ldap-mailhost {enable | disable}
```

```
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	
auth-type {auto | cram-md5 | digest-md5 | login | ntlm | plain}	Enter an authentication type.	auto
access-override {enable | disable}	Enable to override the access profile you specify when you add an administrator with the value of the remote attribute returned from the RADIUS server, if the returned value matches an existing access profile.	disable
access-override-attribute <integer>	Enter the attribute ID of a vender for remote access permission override. The attribute should hold an access profile name that exists on FortiMail. The default ID is 6, which is Fortinet-Access-Profile.	6
access-override-vendor <integer>	Enter the vender's registered RADIUS ID for remote access permission override. The default ID is 12356, which is Fortinet.	12356
option {ssl secure tls senddomain}	Enter one or more of the following in a space-delimited list: • `senddomain`: Enable if the IMAP server requires both the user name and the domain when authenticating. • `ssl`: Enables secure socket layers (SSL) to secure message transmission. • `secure`: Enables secure authentication. • `tls`: Enables transport layer security (TLS) to ensure privacy between communicating application.	
port <port_int>	Enter the TCP port number of the IMAP server. The standard port number for SSL-secured IMAP is 993.	143
server {<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the IMAP server.	
option {ssl secure tls senddomain}	If you want to enable any of the following options, enter them in a space-delimited list: • `domain`: Enable if the POP3 server requires both the user name and the domain when authenticating. • `ssl`: Enables secure socket layers (SSL) to secure message transmission. • `secure`: Enables secure authentication. • `tls`: Enables transport layer security (TLS) to ensure privacy between communicating application.	
port <port_int>	Enter the TCP port number of the POP3 server. The standard port number for SSL-secured POP3 is 995.	110

Variable	Description	Default
server {<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the POP3 server.	
auth-prot {auto | chap | mschap | mschap2 | pap}	Enter the authentication method for the RADIUS server.	mschap2
domain-override {enable | disable}	Enable to override the domain you specify when you add an administrator with the value of the remote attribute returned from the RADIUS server, if the returned value matches an existing protected domain.	disable
domain-override-attribute <integer>	Enter the attribute ID of a vender for remote domain override. The attribute should hold a domain name that exists on FortiMail. The default ID is 3, which is Fortinet-Vdom-Name.	3
domain-override-vendor <integer>	Enter the vender's registered RADIUS ID for remote domain override. The default ID is 12356, which is Fortinet.	12356
nas-ip <ip_addr>	Enter the NAS IP address and Called Station ID (for more information about RADIUS Attribute 31, see RFC 2548 Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address that the FortiMail interface uses to communicate with the RADIUS server will be applied.	0.0.0.0
port <port_int>	If the RADIUS server listens on a nonstandard port number, enter the port number of the RADIUS server.	1812
secret <password_str>	Enter the password for the RADIUS server.	
send-domain {enable | disable}	Enable if the RADIUS server requires both the user name and the domain when authenticating.	disable
server {<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the RADIUS server.	
option {ssl secure tls senddomain}	If you want to enable any of the following options, enter them in a space-delimited list: • `senddomain`: Enable if the SMTP server requires both the user name and the domain when authenticating. • `ssl`: Enables secure socket layers (SSL) to secure message transmission. • `secure`: Enables secure authentication. • `tls`: Enables transport layer security (TLS) to ensure privacy between communicating application	

Variable	Description	Default
server {<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the SMTP server.	
port <port_int>	Enter the TCP port number of the SMTP server. The standard port number for SSL-secured SMTP is 465.	25
try-ldap-mailhost {enable | disable}	Enable if your LDAP server has a mail host entry for the generic user. If you select this option, the FortiMail unit will query the generic LDAP server first to authenticate email users. If no results are returned for the query, the FortiMail unit will query the server you entered in the server field.	enable

Related topics

profile certificate-binding

profile encryption

profile certificate-binding

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

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

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

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

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

Syntax

```
config profile certificate-binding
   edit <profile_id>
      set address-pattern <pattern_str>
      set key-private <key_str>
```

```
        set key-public <key_str>
        set key-usage {both | encryption | signing}
        set password <pwd_str>
end
```

Variable	Description	Default
<profile_id>	Enter the ID number of the certificate binding profile.	
address-pattern <pattern_str>	Enter the email address or domain associated with the identity represented by the personal or server certificate.	
key-private <key_str>	Enter the private key associated with the identity, used to encrypt and sign email from that identity.	
key-public <key_str>	Enter the public key associated with the identity, used to encrypt and sign email from that identity.	
key-usage {both | encryption | signing}	Use the key for encryption, signing, or both.	encryption
password <pwd_str>	Enter the password for the personal certificate files.	

Related topics

profile authentication

profile encryption

profile content

Use this command to create content profiles, which you can use to match email based upon its subject line, message body, and attachments.

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

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

Syntax

```
config profile content
   edit <profile_name>
      [set comment <comment_str>
      set action-default <content-action-profile_name>
      set defersize <KB_int>
      config attachment-scan
         edit <index_int>
```

```
            set action <content-action-profile_name>
            set operator {is | is-not}
            set patterns {archive audio encrypted executable_windows image msoffice openoffice
                 script video}
            set status {enable | disable}
        set scan-options {block-fragmented-email block-password-protected-office bypass-on-smtp-
            auth check-archive-content check-embedded-content check-html-content check-max-num-of-
            attachment check-text-content policy-match}
        set embedded-scan-options {check-msoffice check-msoffice-vba check-msvisio check-openoffice
            check-pdf}
        set max-num-of-attachment <limit_int>
        set max-size-status {enable | disable}
        set max-size-option {message | attachment}
        set max-size <KB_int>
        set action-max-size <content-action-profile_name>
        set action-policy-match <content-action-profile_name>
        set image-analysis-scan {enable | disable}
        set action-image-analysis <content-action-profile_name>
        set decrypt-password-archive {enable | disable}
        set decrypt-password-office {enable | disable}
        set decrypt-password-options {built-in-password-list | user-defined-password-list | words-
            in-email-content}
        set decrypt-password-num-of-words <words_int>
        set action-cdr <content-action-profile_name>
        set html-content-action {convert-to-text | modify-content}
        set html-content-url-action {click-protection | click-protection-isolator | isolator |
            keep | neutralize | remove}
        set html-content-url-selection {tag-attribute tag-content}
        set remove-active-content {enable | disable}
        set text-content-action {click-protection | click-protection-isolator | isolator |
            neutralize | remove-url}
        set cdr-file-type-options {office pdf}
        set archive-scan-options {block-on-failure-to-decompress block-password-protected block-
            recursive}
        set archive-max-recursive-level <threshold_int>
        config monitor
           edit <index_int>
            set action <content-action-profile_name>
            set dict-score <threshold_int>
            set dictionary-group <dictionary-group_name>
            set dictionary-profile <dictionary-profile_name>
            set dictionary-type {group | profile}
            set scan-office {enable | disable}
            set scan-pdf {enable | disable}
            set status {enable | disable}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	
<index_int>	Enter the index number of the attachment scan profile. If the profile does not currently exist, it will be created.	

Variable	Description	Default
action <content-action-profile_name>	Select which content action profile to use for the attachment scan. See profile content-action on page 206.	
operator {is | is-not}	Select either: • `is`: Match the file types that are selected • `is-not`: Match the file types that are **not** selected in patterns {archive audio encrypted executable_windows image msoffice openoffice script video}.	is
patterns {archive audio encrypted executable_windows image msoffice openoffice script video}	Select which file types of attachments will be scanned or omitted from the scan, depending on your configuration of operator {is | is-not}. For multiple file types, separate each entry with a space. This setting applies only if status {enable | disable} is `enable`.	
status {enable | disable}	Enable or disable patterns {archive audio encrypted executable_windows image msoffice openoffice script video} on page 199.	enable
<index_int>	Enter the index number of the content monitoring profile. If the profile does not currently exist, it will be created.	
action <content-action-profile_name>	Select which content action profile to use for the content monitor scan. See profile content-action on page 206.	
dict-score <threshold_int>	Enter the number of times that an email must match the content monitor profile before it will receive the antispam action.	1
dictionary-group <dictionary-group_name>	Enter the dictionary profile group that this content monitor profile will use. See profile dictionary-group on page 214. The FortiMail unit will compare content in the subject line and message body of the email message with words and patterns in the dictionary profiles. If it locates matching content, the FortiMail unit will perform the actions configured for this monitor profile. For information on dictionary profiles, see the FortiMail Administration Guide.	
dictionary-profile <dictionary-profile_name>	Enter the dictionary profile that this content monitor profile will use. The FortiMail unit will compare content in the subject line and message body of the email message with words and patterns in the dictionary profile. If it locates matching content, the FortiMail unit will perform the actions configured for this monitor profile in profile content-action on page 206. For information on dictionary profiles, see the FortiMail Administration Guide.	

Variable	Description	Default
dictionary-type {group | profile}	Select either: • `profile`: Detect content based upon a dictionary profile. Also configure dictionary-profile <dictionary-profile_name>. • `group`: Detect content based upon a group of dictionary profiles. Also configure dictionary-group <dictionary-group_name>.	group
scan-office {enable | disable}	Enable or disable Microsoft Word document scanning for this profile.	disable
scan-pdf {enable | disable}	Enable or disable PDF document scanning for this profile.	disable
status {enable | disable}	Enable or disable this monitor profile.	disable
action-cdr <content-action-profile_name>	Select the action profile to use for CDR. See also profile content-action on page 206.	
action-default <content-action-profile_name>	Select a content action profile. See profile content-action on page 206. This default setting applies only to sub-scans that do not have their own individually configured action, such as action-cdr <content-action-profile_name>.	
action-image-analysis <content-action-profile_name>	For the `image` email file type, you can use a content action profile to override action-default <content-action-profile_name>.	
action-max-size <content-action-profile_name>	Select the content action profile to use if an email or attachment exceeds max-size <KB_int>.	
archive-max-recursive-level <threshold_int>	Enter the nesting depth threshold. Depending upon each attached archive's depth of archives nested within the archive, the FortiMail unit will use one of the following methods to determine whether it should block or pass the email. • **If the `archive-max-recursive-level` is `0`, or attachment's depth of nesting is equal to or less than `archive-max-recursive-level`:** If the attachment contains a file that matches one of the other file types, perform the action configured for that file type, either block or pass. • **If the attachment's depth of nesting is greater than `archive-max-recursive-level`**: Apply the block action, unless you have not selected `block-recursive` in archive-scan-options {block-on-failure-to-decompress block-password-protected block-recursive}, in which case it will pass the file type content filter. Block actions are specified in the profile content-action on page 206.	12

Variable	Description	Default
	This setting applies only if `pcheck-archive-content` is selected in scan-options {block-fragmented-email block-password-protected-office bypass-on-smtp-auth check-archive-content check-embedded-content check-html-content check-max-num-of-attachment check-text-content policy-match}.	
action-policy-match <content-action-profile_name>	Select the content action profile to use if an email triggers a policy match. This setting applies only if `policy-match` is selected in scan-options {block-fragmented-email block-password-protected-office bypass-on-smtp-auth check-archive-content check-embedded-content check-html-content check-max-num-of-attachment check-text-content policy-match}.	
archive-scan-options {block-on-failure-to-decompress block-password-protected block-recursive}	Select what option(s) to use when scanning archives: • `block-on-failure-to-decompress`: Apply the action configured in profile content-action on page 206 if an attached archive cannot be successfully decompressed in order to scan its contents. • `block-password-protected`: Apply the action configured inprofile content-action on page 206 if an attached archive is password-protected. • `block-recursive`: Block archive attachments whose depth of nested archives exceeds the value defined under archive-max-recursive-level <threshold_int>. Separate multiple options with a space. This setting applies only if `check-archive-content` is selected in scan-options {block-fragmented-email block-password-protected-office bypass-on-smtp-auth check-archive-content check-embedded-content check-html-content check-max-num-of-attachment check-text-content policy-match}.	
cdr-file-type-options {office pdf}	Select which file type(s) to apply content disarming and reconstruction (CDR) to: • `office`: Microsoft Office files. • `pdf`: PDF files. See also file content-disarm-reconstruct on page 109.	
comment <comment_str>	Enter a descriptive comment.	
decrypt-password-archive {enable | disable}	Enable or disable to decrypt password protected archives. Also configure decrypt-password-options {built-in-password-list | user-defined-password-list | words-in-email-content}.	disable
decrypt-password-num-of-words <words_int>	Enter the number of words adjacent to the keyword to try for file decryption.	5

Variable	Description	Default
	For example, in an email, there could be a sentence such as: “To open the document, please use password 123456. If you cannot open it, please contact us.” If you specify to use two words before and after the keyword, then “please”, “use” (two words before the keyword “password”), “123456”, and “If” (two words after the keyword “password”) would be used as one by one as the password to decrypt the attachments. If no keyword exists, any words in the email body may be tried as the password.	
decrypt-password-office {enable | disable}	Enable to decrypt password protected Microsoft Office files. Also configure decrypt-password-options {built-in-password-list | user-defined-password-list | words-in-email-content}.	disable
decrypt-password-options {built-in-password-list | user-defined-password-list | words-in-email-content}	Select which kind of password to use to decrypt files. This setting applies only if decrypt-password-archive {enable | disable}is `enable` and you have configured file decryption password on page 110.	words-in-email-content
defersize <KB_int>	Enter the attachment size threshold in kilobytes for deferred delivery. To disable the limit, enter `0`. See also defer-delivery-starttime <time_str> on page 330 and defer-delivery {enable | disable}. **Tip:** Alternatively, configure max-size <KB_int>.	0
embedded-scan-options {check-msoffice check-msoffice-vba check-msvisio check-openoffice check-pdf}	Specify which option(s) to use when scanning documents with embedded files. • `check-msoffice`: Scan embedded files in Microsoft Office documents. • `check-msoffice-vba`: Scan embedded files in Microsoft Office Visual Basic documents. • `check-msvisio`: Scan embedded files in Microsoft Visio documents. • `check-openoffice`: Scan embedded files in OpenOffice.org documents. • `check-pdf`: Scan embedded files in PDF documents. Similar to an archive, documents can sometimes contain video, graphics, sounds, and other files that are used by the document. By wrapping files within a document instead of linking to the file on a separate, external location, a document becomes more portable. However, it also means that documents with other files embedded can be used to hide infected files.	
html-content-action {convert-to-text | modify-content}	Select either: • `convert-to-text`: Convert hypertext markup language (HTML) email to plain text. • `modify-content`: Modify the HTML content, using the CDR settings such as html-content-url-action {click-protection | click-protection-isolator | isolator | keep | neutralize | remove}, html-content-url-selection {tag-	modify-content

Variable	Description	Default
	attribute tag-content}, and remove-active-content {enable | disable}. This setting applies only if `check-html-content` is selected in scan-options {block-fragmented-email block-password-protected-office bypass-on-smtp-auth check-archive-content check-embedded-content check-html-content check-max-num-of-attachment check-text-content policy-match}.	

html-content-url-action {click-protection | click-protection-isolator | isolator | keep | neutralize | remove}	If html-content-action {convert-to-text | modify-content} is `modify-content`, select how FortiMail will modify the HTML:
	• `click-protection`: Rewrite the URL. If the user clicks on the URL, perform the click protection action configured in system fortiguard url-protection on page 305.
	• `click-protection-isolator`: Rewrite the URL and if the user clicks on it, redirect the URL to FortiMail for scanning. If the URL is malicious, it will be blocked; if the URL passes the scan, then it is rewritten to point to FortiIsolator, and the user will browse through FortiIsolator.
	• `isolator`: Redirect the user to FortiIsolator so that the user will be browsing indirectly, protected through FortiIsolator.
	• `keep`: Keep the URL or script. Do not remove or modify it.
	• `neutralize`: Modify the URL to make it inactive when clicked, but still easy to determine what the original URL was. For example, a link to:
	`https://www.example.com`
	is changed to:
	`hxxps:\\www[.]example[.]com`
	• `remove`: Remove the URL or script.
	This setting applies only if `check-html-content` is selected in scan-options {block-fragmented-email block-password-protected-office bypass-on-smtp-auth check-archive-content check-embedded-content check-html-content check-max-num-of-attachment check-text-content policy-match}.
		click-protection

html-content-url-selection {tag-attribute tag-content}	Select where CDR modifications should apply: • `tag-attribute`: HTML tag attributes. For example, modify the `href` attribute in hyperlinks such as in `<a href="https://example.com/">`. • `tag-content`: HTML tag text contents. Separate multiple options with a space. This setting applies only if html-content-action {convert-to-text | modify-content} is `modify-content`.	tag-attribute
image-analysis-scan {enable | disable}	If you have purchased the image scan feature license, you can enable the scan for image categories that you may want to block, such as violence and adult images. You can also configure the scan sensitivity and image fie size threshold. Seeantispam image-analysis on page 48.	disable
max-num-of-attachment <limit_int>	Enter how many attachments are allowed in one email message. The valid range is from 1 to 100.	10

Variable	Description	Default
	This setting applies only if `check-max-num-of-attachment` is selected in scan-options {block-fragmented-email block-password-protected-office bypass-on-smtp-auth check-archive-content check-embedded-content check-html-content check-max-num-of-attachment check-text-content policy-match}.	
max-size <KB_int>	Enter the maximum size threshold in kilobytes. Also configure action-max-size <content-action-profile_name>. To disable deferred delivery, enter `0`. This setting applies only if max-size-status {enable | disable} is `enable`.	10240
max-size-option {message | attachment}	Select to apply max-size <KB_int> to either the body of the email message or attachments.	message
max-size-status {enable | disable}	Enable to apply max-size <KB_int>.	disable

remove-active-content {enable | disable}	Enable to remove active content such as JavaScript.
	This setting applies only if html-content-action {convert-to-text | modify-content} is `modify-content`.
	Caution: If you want to convert HTML to plain text, then you must also enable replace-content {enable | disable} on page 210. Otherwise, the FortiMail unit will keep the HTML tags and only apply whichever other action(s) in the content action profile.
	If you enable replace-content {enable | disable}, then all HTML tags will be removed, except for the minimum required by the HTML document type definition (DTD):
	• `<html>`
	• `<head>`
	• `<body>`
	Body text will be stripped of other surrounded by `<pre>` tags, which is typically rendered in a monospace font, causing the appearance to mimic plain text.
	For linked files, which are hosted on an external web server for subsequent download rather than directly embedded or attached to the email, the FortiMail unit will download and attach the file to the email **before** removing the `<img>` or `<embed>` tag. In this way, while the format is converted to plain text, attachments and linked files which may be relevant to the content are still preserved.
	For example, in an email that is a mixture of HTML and plain text (`Content-Type: multipart/alternative`), and if replace-content {enable | disable} is `enable`, the FortiMail unit would remove hyperlink, font, and other HTML tags in the sections labeled with `Content-Type: text/html`. Linked images would be converted to attachments. The MIME `Content-Type: text/html` label itself, however, would **not** be modified.
		enable

Variable	Description	Default
scan-options {block-fragmented-email block-password-protected-office bypass-on-smtp-auth check-archive-content check-embedded-content check-html-content check-max-num-of-attachment check-text-content policy-match}	Select which option(s) to use: • `block-fragmented-email`: Detect and block fragmented email. Some mail user agents, such as Microsoft Outlook, can fragment big emails into multiple sub-messages. This is used to bypass oversize limits and scanning. • `block-password-protected-office`: Detect if an attached Microsoft Office document is password-protected, and cannot be decompressed in order to scan its contents. Apply the block or other action selected in the content action profile. • `bypass-on-smtp-auth`: Omit antispam scans when an SMTP sender is authenticated. • `check-archive-content`: Scan archives. Also configure archive-max-recursive-level <threshold_int> etc. • `check-embedded-content`: Scan embedded files. Documents, similar to an archive, can sometimes contain video, graphics, sounds, and other files that are used by the document. By embedding the required file within itself instead of linking to such files externally, a document becomes more portable. However, it also means that documents can be used to hide infected files that are the real attack vector. • `check-html-content`: Detect hypertext markup language (HTML) email and perform content disarming and reconstruction (CDR). FortiMail will also add: `X-FEAS-ATTACHMENT-FILTER: Contains HTML tags.` to the message headers. Also configure action-cdr <content-action-profile_name>etc. • `check-max-num-of-attachment`: Limit the number of attaches. Also configure max-num-of-attachment <limit_int> . • `check-text-content`: Detect URLs and perform content disarming and reconstruction (CDR) in plain text email. Also configure action-cdr <content-action-profile_name> and text-content-action {click-protection | click-protection-isolator | isolator | neutralize | remove-url}. • `policy-match`: Defer mail delivery from specific senders configured in the policy. By sending low-priority, bandwidth-consuming email such as newsletter digest or marketing campaigns at scheduled times, you can conserve bandwidth at peak time so that high priority email can be sent more quickly. See also mailsetting preference on page 126 and action-policy-match <content-action-profile_name> on page 201. Separate multiple options with a space.	

Variable	Description	Default

text-content-action {click-protection | click-protection-isolator | isolator | neutralize | remove-url}	Select how FortiMail will modify the HTML:
	• `click-protection`: Rewrite the URL. If the user clicks on the URL, perform the click protection action configured in system fortiguard url-protection on page 305.
	• `click-protection-isolator`: Rewrite the URL and if the user clicks on it, redirect the URL to FortiMail for scanning. If the URL is malicious, it will be blocked; if the URL passes the scan, then it is rewritten to point to FortiIsolator, and the user will browse through FortiIsolator.
	• `isolator`: Redirect the user to FortiIsolator so that the user will be browsing indirectly, protected through FortiIsolator.
	• `neutralize`: Modify the URL to make it inactive when clicked, but still easy to determine what the original URL was. For example, a link to:
	`https://www.example.com`
	is changed to:
	`hxxps:\\www[.]example[.]com`
	• `remove-url`: Remove the URL.
	This setting applies only if `check-text-content` is selected in scan-options {block-fragmented-email block-password-protected-office bypass-on-smtp-auth check-archive-content check-embedded-content check-html-content check-max-num-of-attachment check-text-content policy-match}.
		click-protection

Related topics

antispam image-analysis
file content-disarm-reconstruct
file decryption password
profile content-action
system fortiguard url-protection

profile content-action

Use this command to define content action profiles. Content action profiles can be used to apply content-based encryption.

Alternatively, content action profiles can define one or more things that the FortiMail unit should do if the content profile determines that an email contains prohibited words or phrases, file names, or file types.

For example, you might have configured most content profiles to match prohibited content, and therefore to use a content action profile named `quar_profile` which quarantines email to the system quarantine for review.

However, you have decided that email that does not pass the dictionary scan named `financial_terms` is **always** prohibited, and should be rejected so that it does not require manual review. To do this, you would first configure a second action profile, named `rejection_profile`, which rejects email. You would then override

`quar_profile` specifically for the dictionary-based content scan in each profile by selecting `rejection_profile` for content that matches `financial_terms`.

Syntax

```
config profile content-action
   edit <profile_name>
      [set comment "<comment_str>"]
      config header-insertion-list
         edit <header-insertion-name <header-key>>
            set header-insertion-value <header-value_str>
      end
      config header-removal-list
         edit <header-removal-name <header-key_str>>
         next
      end
      set action {discard | domain-quarantine | encryption | none | personal-quarantine |
           reject | rewrite-rcpt | system-quarantine | treat-as-spam}
      set alternate-host-status {enable | disable}
      set alternate-host {<relay_fqdn> | <relay_ipv4>}
      set archive-status {enable | disable}
      set archive-account <account_name>
      set bcc-status {enable | disable}
      set bcc-addr <recipient_email>
      set bcc-env-from-addr <bcc-sender_email>
      set bcc-env-from-status {enable | disable}
      set defer-delivery {enable | disable}
      set deliver-to-original-host {enable | disable}
      set disclaimer-insertion {enable | disable}
      set disclaimer-insertion-content <message_name>
      set disclaimer-insertion-location {beginning | end}
      set fortiguard-antispam-outbreak {enable | disable}
      set notification-status {enable | disable}
      set notification-profile <profile_name>
      set quarantine-folder "<path_str>"
      set quarantine-notify {enable | disable}
      set quarantine-notify-profile <profile_name>
      set remove-header {enable | disable}
      set replace-content {enable | disable}
      set replacement-message <profile_name>
      set rewrite-rcpt-domain-type {none | prefix | replace | suffix}
      set rewrite-rcpt-domain-value <text_str>
      set rewrite-rcpt-local-type {none | prefix | replace | suffix}
      set rewrite-rcpt-local-value <value_str>
      set subject-tagging-text "<text_str>"
      set tagging type {insert-header | tag-subject}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile. To view a list of existing entries, enter a question mark (?).	

Variable	Description	Default
action {discard | domain-quarantine | encryption | none | personal-quarantine | reject | rewrite-rcpt | system-quarantine | treat-as-spam}	Enter the action that the FortiMail unit will perform if the content profile determines that an email contains prohibited words or phrases, file names, or file types. • `discard`: Accept the email, but then delete it instead of delivering the email, without notifying the SMTP client. • `domain-quarantine`: Enter to redirect email to the per-domain quarantine. For more information, see the FortiMail Administration Guide. Note that this option is only available with a valid advanced management license. • `encryption`: Apply an encryption profile. • `none`: Apply any configured header or subject line tags, if any. • `personal-quarantine`: Divert the email to the per-recipient quarantine. • `reject`: Reject the email, replying with an SMTP error code to the SMTP client. • `rewrite-rcpt`: Enter to change the recipient address of any email that matches the content profile. Also configure rewrite-rcpt-domain-type {none | prefix | replace | suffix}, rewrite-rcpt-domain-value <text_str>, rewrite-rcpt-local-type {none | prefix | replace | suffix}, and rewrite-rcpt-local-value <value_str>. • `system-quarantine`: Divert the email to the system quarantine. • `treat-as-spam`: Apply the action selected in the antispam profile.	none
alternate-host {<relay_fqdn> | <relay_ipv4>}	Type the fully qualified domain name (FQDN) or IP address of the alternate relay or SMTP server. This field applies only if `alternate-host-status` is `enable`.	
archive-account <account_name>	Type the email archive account name where you want to archive the email. For more information about archive accounts, see archive policy on page 65.	
archive-status {enable | disable}	Enable or disable use of archive-account <account_name>.	disable
alternate-host-status {enable | disable}	Enable to route the email to a specific SMTP server or relay. Also configure alternate-host {<relay_fqdn> | <relay_ipv4>}. **Note:** If you enable this setting, for all email that matches the profile, the FortiMail unit will use this destination and ignore mailsetting relay-host-list and the protected domain's tp-use-domain-mta {yes | no}.	disable
bcc-addr <recipient_email>	Type the blind carbon copy (BCC) recipient email address. This field applies only if `bcc-status` is `enable`.	

Variable	Description	Default
bcc-env-from-addr <bcc-sender_email>	Specify an envelope from BCC address. In the case that email is not deliverable and bounced back, the email is returned to the specified envelope from address instead of the original sender. This is helpful when you want to use a specific email to collect bounce notifications. This field applies only if `bcc-env-from-status` is `enable`.	
bcc-env-from-status {enable | disable}	Enable to specify an envelope from address.	disable
bcc-status {enable | disable}	Enable to send a BCC of the email. Also configure suspicious-newsletter-status {enable | disable}.	disable
comment "<comment_str>"	Enter a description or comment.	
defer-delivery {enable | disable}	Enable to defer delivery of emails that may be resource intensive and reduce performance of the mail server, such as large email messages, or lower priority email from certain senders (for example, marketing campaign email and mass mailing). See also defer-delivery-starttime <time_str> on page 330.	disable
deliver-to-original-host {enable | disable}	Enable to deliver the message to the original host.	disable
disclaimer-insertion {enable | disable}	Enable to insert disclaimer.	disable
disclaimer-insertion-content <message_name>	Specify the content name to be inserted.	default
disclaimer-insertion-location {beginning | end}	Insert the disclaimer at the beginning or end of the message.	beginning
fortiguard-antispam-outbreak {enable | disable}	Enable or disable FortiGuard antispam outbreak action, sending incoming email to the deferred mail queue.	disable
header-insertion-name <header-key>	Enter the message header key. The FortiMail unit will add this text to the message header of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes based on text appearing in various parts of email messages, including the message header. For details, see the documentation for your email client. Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter: `X-Content-Filter: Contains banned word.` If you enter a header line that does not include a colon, the FortiMail unit will automatically append a colon, causing the entire text that you enter to be the key. **Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.	

Variable	Description	Default
	Also configure tagging type {insert-header | tag-subject}.	
header-removal-name <header-key_str>	Enter the message header name to be removed.	
header-insertion-value <header-value_str>	Enter the message header value. The FortiMail unit will add this value to the message header of the email before forwarding it to the recipient. Also configure tagging type {insert-header | tag-subject}.	
notification-profile <profile_name>	Type the name of the notification profile used for sending notifications.	
notification-status {enable | disable}	Enable sending notifications using a notification profile.	disable
quarantine-folder "<path_str>"	Enter the location of the quarantine folder.	disable
quarantine-notify {enable | disable}	Enable to quarantine and also notify the recipient about the action.	disable
quarantine-notify-profile <profile_name>	Enter the name of a notification profile.	
remove-header {enable | disable}	Enable removing headers defined in the header removal list. Once enabled, configure header-removal-name <header-key_str> under `config header-removal-list`.	disable
replace-content {enable | disable}	Enable or disable replacement of the contents of the email.	disable
replacement-message <profile_name>	Enter the name of the custom message for replacement of the contents of the email.	
rewrite-rcpt-domain-type {none | prefix | replace | suffix}	Change the domain part (the portion of the email address after the '@' symbol) of the recipient address of any email that matches the content profile. • `none`: No change. • `prefix`: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <text_str>. • `suffix`: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <text_str>. • `replace`: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <text_str>.	none
rewrite-rcpt-domain-value <text_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-domain-type {none | prefix | replace | suffix}.	
rewrite-rcpt-local-type {none | prefix | replace | suffix}	Change the local part (the portion of the email address before the '@' symbol, typically a user name) of the recipient address of any email that matches the content profile. • `none`: No change. • `prefix`: Enter to prepend the part with new text. Also	none

Variable	Description	Default
	configure rewrite-rcpt-local-value <value_str>. • `suffix`: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>. • `replace`: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str>.	
rewrite-rcpt-local-value <value_str>	Enter the text for the option (except none) you choose in rewrite-rcpt-local-type {none | prefix | replace | suffix}.	
subject-tagging-text "<text_str>"	Enter the text that will appear in the subject line of the email, such as `[PROHIBITED-CONTENT]`. The FortiMail unit will prepend this text to the subject line of the email before forwarding it to the recipient. Many email clients can sort incoming email messages into separate mailboxes based on text appearing in various parts of email messages, including the subject line. For details, see the documentation for your email client. Also configure tagging type {insert-header | tag-subject}.	
tagging type {insert-header | tag-subject}	Enter the type of tagging for this profile.	

Related topics

profile encryption

profile cousin-domain

Use this command to mitigate business email compromise (BEC) email-impersonation risks. Domain names may be deliberately misspelled, either by character removal, substitution, and/or transposition, in order to make emails look as though they originate from trusted internal sources.

Configure cousin domains to define those domain names that should be subjected to cousin domain scanning and those domains that are exempt from scanning.

Once created, cousin domain profiles can be referenced in antispam profiles. In addition, cousin domain scan options can be set within antispam profiles. See cousin-domain-scan-option {auto-detection body-detection header-detection}.

Syntax

```
config profile cousin-domain
   edit <profile_name>
      config entry
         edit <entry_int>
```

```
            set domain-name <string>
            set domain-name-type {wildcard | regex}
         next
      end
      config exempt
         edit <exempt_int>
            set domain-name <string>
            set domain-name-type {wildcard | regex}
         next
      end
end
```

Variable	Description	Default
<profile_name>	Enter the name of the cousin profile.	
<entry_int>	Enter the entry number of the cousin domain profile. If the entry profile does not currently exist, it will be created.	
<exempt_int>	Enter the entry number of the cousin domain profile. If the exempt profile does not currently exist, it will be created.	
domain-name <string>	Enter the domain name string of the entry rule/exempt rule either as a wildcard or regular expression.	
domain-name-type {wildcard | regex}	Select the domain name type of the entry rule/exempt rule.	regex

profile dictionary

Use this command to configure dictionary profiles.

Unlike banned words, dictionary terms are UTF-8 encoded, and may include characters other than US-ASCII characters, such as é or ñ.

Dictionary profiles can be grouped or used individually by antispam or content profiles to detect spam, banned content, or content that requires encryption to be applied.

Syntax

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

```
            set pattern-max-limit {enable | disable}
    end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile.	
<item_int>	Enter the index number for the pattern entry where you can add a word or phrase to the dictionary.	
pattern <pattern_str>	For a predefined pattern, enter a value to change the predefined pattern name. For a use-defined pattern, enter a word or phrase that you want the dictionary to match, expressed either verbatim, with wild cards, or as a regular expression. Regular expressions do not require slash (`/`) boundaries. For example, enter: `v[i1]agr?a` Matches are case insensitive and can occur over multiple lines as if the word were on a single line (that is, Perl-style match modifier options `i` and `s` are in effect). The FortiMail unit will convert the encoding and character set into UTF-8, the same encoding in which dictionary patterns are stored, before evaluating an email for a match with the pattern. Because of this, your pattern must match the UTF-8 string, not the originally encoded string. For example, if the original encoded string is: `=?iso-8859-1?B?U2UgdHJhdGEgZGVsIHNwYW0uCg==?=` the pattern must match: `Se trata del spam.` Entering the pattern `*iso-8859-1*` would **not** match.	
pattern-comments <comment_str>	Enter any description for the pattern.	
pattern-type {ABAROUTING | CANSIN | CUSIP | CreditCard | ISIN | USSSN | regex | wildcard}	Enter `ABAROUTING`, `CANSIN`, `CUSIP`, `CreditCard`, `ISIN`, or `USSSN` for predefined patterns. • `ABAROUTING`: A routing transit number (RTN) is a nine digit bank code, used in the United States, which appears on the bottom of negotiable instruments such as checks identifying the financial institution on which it was drawn. • `CANSIN`: Canadian Social Insurance Number. The format is three groups of three digits, such as 649 242 666. • `CUSIP`: CUSIP typically refers to both the Committee on Uniform Security Identification Procedures and the 9-character alphanumeric security identifiers that they distribute for all North American securities for the purposes of facilitating clearing and settlement of trades. • `CreditCard`: Major credit card number formats. • `ISIN`: An International Securities Identification Number (ISIN) uniquely identifies a security. Securities for which ISINs are issued include bonds, commercial paper, equities and warrants. The ISIN code is a 12-character alpha-numerical code that does not contain information characterizing financial instruments but serves for uniform identification of a security at	regex

Variable	Description	Default
	trading and settlement. • `USSSN`: United States Social Security number. The format is a nine digit number, such as 078051111. • For user-defined patterns, enter either: • `wildcard`: Pattern is verbatim or uses only simple wild cards (`?` or `*`). • `regex`: Pattern is a Perl-style regular expression.	
pattern-weight <weight_int>	Enter a number by which an email's dictionary match score will be incremented for each word or phrase it contains that matches this pattern. The dictionary match score may be used by content monitor profiles to determine whether or not to apply the content action.	1
pattern-scan-area {header | body}	Enter `header` to match occurrences of the pattern when it is located in an email's message headers, including the subject line, or `body` to match occurrences of the pattern when it is located in an email's message body.	
pattern-status {enable | disable}	Enable or disable a pattern in a profile.	disable
pattern-max-weight <weight_int>	Enter the maximum by which matches of this pattern can contribute to an email's dictionary match score.	1
pattern-max-limit {enable | disable}	Enable if the pattern must not be able to increase an email's dictionary match score more than the amount configured in pattern-max-weight <weight_int>.	disable

Related topics

profile dictionary-group

profile dictionary-group

Use this command to create groups of dictionary profiles.

Dictionary groups can be useful when you want to use multiple dictionary profiles during the same scan.

For example, you might have several dictionaries of prohibited words — one for each language — that you want to use to enforce your network usage policy. Rather than combining the dictionaries or creating multiple policies and multiple content profiles to apply each dictionary profile separately, you could simply group the dictionaries, then select that group in the content monitor profile.

Before you can create a dictionary group, you must first create one or more dictionary profiles. For more information about dictionary profiles, see profile dictionary on page 212.

Syntax

```
config profile dictionary-group
   edit <group_name>
      config dictionaries
         edit <dictionary_name>
end
```

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

Related topics

profile dictionary

profile dlp

Use this command to add scan rules/conditions to Data Loss Prevention (DLP) profiles. Specify what actions to take and then apply DLP profiles to IP or recipient based policies.

Syntax

```
config profile dlp
   edit <profile name>
      config content-scan
         edit <rule_order>
            set action {Discard | Encrypt_Pull | Reject | Replace | SystemQuarantine |
                 UserQuarantine}
            set name <scan_rule_name>
            set status {enable | disable}
      end
      set comment <string>
      set action-default {Discard | Encrypt_Pull | Reject | Replace | SystemQuarantine |
           UserQuarantine}
end
```

Variable	Description	Default
action {Discard | Encrypt_Pull | Reject | Replace | SystemQuarantine | UserQuarantine}	Specify the action for this rule.	
name <scan_rule_name>	Enter a scan rule name.	

Variable	Description	Default
status {enable | disable}	Enable or disable this rule.	enable
comment <string>	Enter optional comments for the profile.	
action-default {Discard | Encrypt_Pull | Reject | Replace | SystemQuarantine | UserQuarantine}	Specify the default action for this profile.	

profile email-address-group

Use this command to create groups of email addresses.

Email groups include groups of email addresses that are used when configuring access control rules. For information about access control rules, see cloud-api profile antivirus on page 76.

Syntax

```
config profile email-address-group
   edit <group_name>
      config member
         edit <email_address>
end
```

Variable	Description	Default
<group_name>	Enter the name of the email address group.	
<email_address>	Enter the email address that you want to include in the email group.	

Related topics

cloud-api profile antivirus

profile encryption

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

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

Syntax

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

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

Related topics

profile authentication

system global

profile geoip-group

Use this command to create groups of IP addresses organized by geographic locations such as country names, using the GeoIP database from FortiGuard.

The database combines public IP address range, owner, service port numbers, and security credibility. Information is regularly added to this database, such as updates to geographic location, IP reputation, popularity, DNS entries, and more. All this information can help to keep your Internet security configuration up-to-date as cloud and other services move and expand.

Syntax

```
config profile geoip-group
   edit name <group_name>
      [set description "<description_str>"]
      set country {ZZ O1 AD ...}
end
```

Variable	Description	Default
name <group_name>	Enter a unique name.	
description "<description_str>"	Enter a description.	
country {ZZ O1 AD ...}	Enter a country code. Separate multiple countries with a space. To display a list of currently known country codes, enter: `set country ?`	

Related topics

system geoip-override

policy access-control delivery

policy access-control receive

policy ip

profile impersonation

Email impersonation is one of the email spoofing attacks. It forges the email header to deceive the recipient because the message appears to be from a different source than the actual address.

To fight against email impersonation, you can map high valued target display names with correct email addresses and FortiMail can check for the mapping. For example, an external spammer wants to impersonate the CEO of your company(ceo@company.com). The spammer will put "CEO ABC <ceo@external.com>" in the

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

You can also add empt entries to force the FortiMail to skip impersonation analysis.

There are two ways to do the mapping:

- **Manual**: you manually enter mapping entries and create impersonation analysis profiles as described below.
- **Dynamic**: FortiMail Mail Statistics Service can automatically learn the mapping.

Syntax

```
config impersonation
   edit <name>
      config entry
         edit <entry>
            set display-name
            set display-name-type
            set email-address
      config exempt
         edit <entry>
            set display-name
            set display-name-type
            set email-address
end
```

Variable	Description	Default
<name>	Enter the profile name.	
<entry>	Enter the profile entry	
display-name	Enter the display name to be mapped to the email address. You can use the wildcard or regular expression.	
display-name-type	Enter the display name pattern	
email-address	Enter the email address to be mapped to the display name. The email address can be from protected/internal domains or unprotected/external domains.	

profile ip-address-group

Use this command to create groups of IP addresses.

IP groups include groups of IP addresses that are used when configuring access control rules. For information about access control rules, see cloud-api profile antivirus on page 76.

Syntax

```
config profile ip-address-group
   edit <group_name>
      [set comment "<comment_str>"]
      config member
         edit {<host_ipv4/mask> | <host_ipv4range>}
end
```

Variable	Description	Default
<group_name>	Enter the name of the IP address group.	
comment "<comment_str>"	Enter a description or comment.	
{<host_ipv4/mask> | <host_ipv4range>}	Enter the IP address and netmask that you want to include in the group. For example, enter `10.10.10.10/24` or `10.10.10.0-10.10.10.255` to match a 24-bit subnet, or all addresses starting with `10.10.10`. This will appear as `10.10.10.0/24` in objects that use the group such as access rules, with the `0` indicating that any value is matched in that position of the address. Similarly, `10.10.10.10/32` matches only the `10.10.10.10` IP address. To match any address, enter `0.0.0.0/0`.	

Related topics

cloud-api profile antivirus

profile ip-pool

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

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

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

For more information, see the FortiMail Administration Guide.

Syntax

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

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

profile ldap

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

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

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

Syntax

```
config profile ldap
   edit <profile_name>
      [set comment "<comment_str>"]
      set access-override {enable | disable}
      set access-override-attribute <attribute_str>
      set address-map-state {enable | disable}
      set alias-base-dn <dn_str>
      set alias-bind-dn <bind_dn_str>
      set alias-bind-password <bindpw_str>
      set alias-dereferencing {never | always | search | find}
      set alias-expansion-level <limit_int>
      set alias-group-expansion-state {enable | disable}
      set alias-group-member-attribute <attribute_str>
      set alias-group-query <query_str>
      set alias-member-mail-attribute <attribute_str>
      set alias-member-query <query_str>
      set alias-schema {activedirectory | dominoperson | inetlocalmailrcpt | inetorgperson |
            userdefined}
```

```
set alias-scope {base one | sub}
set alias-state {enable | disable}
set antispam <attribute_str>
set antivirus <attribute_str>
set asav-state {enable | disable}
set auth-bind-dn {cnid | none | searchuser | upn}
set authstate {enable | disable}
set base-dn <base-dn_str>
set bind-dn <bind-dn_str>
set bind-password <bind-password_str>
set cache-state {enable | disable}
set cache-ttl <ttl_int>
set chain <ldap-profile_name>
set chain-status {enable | disable}
set client-cert-auth {enable | disable}
set client-cert <certificate_name>
set cnid-name <cnid_str>
set content <content-profile_name>
set dereferencing {never | always | search | find}
set display-name <display-name_str>
set domain-antispam-attr <attribute_str>
set domain-antivirus-attr <attribute_str>
set domain-content-attr <attribute_str>
set domain-override {enable | disable}
set domain-override-attribute <attribute_str>
set domain-parent-attr <attribute_str>
set domain-query <query_str>
set domain-routing-mail-host-attr <attribute_str>
set domain-state {enable | disable}
set external-address <attribute_str>
set fallback-port <port_int>
set fallback-server {<server_fqdn> | <server_ipv4>}
set group-base-dn <base-dn_str>
set group-expansion-level {1..6}
set group-membership-attribute <attribute_str>
set group-name-attribute <attribute_str>
set group-owner {enable | disable}
set group-owner-address-attribute <attribute_str>
set group-owner-attribute <attribute_str>
set group-relative-name {enable | disable}
set group-virtual {enable | disable}
set groupstate {enable | disable}
set internal-address <attribute_str>
set port <port_int>
set query <query_str>
set rcpt-vrfy-bypass {enable | disable}
set referrals-chase {enable | disable}
set routing-mail-host <attribute_str>
set routing-mail-addr <attribute_str>
set routing-state {enable | disable}
set schema {activedirectory | dominoperson | inetlocalmailrcpt | inetorgperson |
    userdefined}
set scope {base | one | sub}
set secure {none | ssl}
set server {<server_fqdn> | <server_ipv4> | <server_ipv6>
set timeout <timeout_int>
set unauth-bind {enable | disable}
```

```
        set upn-suffix <upns_str>
        set user-display-name-attr <attribute_str>
        set user-display-name-retrieval {enable | disable}
        set version {ver2 | ver3}
        set webmail-password-change {enable | disable}
        set webmail-password-schema {openldap | activedirectory}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the LDAP profile.	
access-override {enable | disable}	Enable to override the access profile you specify when you add an administrator with the value of the remote attribute returned from the LDAP server, if the returned value matches an existing access profile. If there is no match, the specified access profile will still be used. Also specify the access profile attribute.	disable
access-override-attribute <attribute_str>	Specify the access profile attribtue.	
address-map-state {enable | disable}	Enable to query the LDAP server defined in the LDAP profile for user objects' mappings between email addresses.	disable
alias-base-dn <dn_str>	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail will search for either alias or user objects. User or alias objects should be child nodes of this location. Whether you should specify the base DN of either user objects or alias objects varies by your LDAP schema style. Schema may resolve alias email addresses directly or indirectly (using references). Direct resolution: Alias objects directly contain one or more email address attributes, such as `mail` or `rfc822MailMember`, whose values are user email addresses such as `user@example.com`, and that resolves the alias. The Base DN, such as `ou=Aliases,dc=example,dc=com`, should contain alias objects.	

Variable	Description	Default
	Indirect resolution: Alias objects do **not** directly contain an email address attribute that can resolve the alias; instead, in the style of LDAP group-like objects, the alias objects contain only references to user objects that are “members” of the alias “group.” User objects’ email address attribute values, such as `user@example.com`, actually resolve the alias. Alias objects refer to user objects by possessing one or more “member" attributes whose value is the DN of a user object, such as `uid=user,ou=People,dc=example,dc=com`. The FortiMail unit performs a first query to retrieve the distinguished names of “member" user objects, then performs a second query using those distinguished names to retrieve email addresses from each user object. The Base DN, such as `ou=People,dc=example,dc=com`, should contain user objects.	
alias-bind-dn <bind_dn_str>	Enter the bind DN, such as `cn=FortiMailA,dc=example,dc=com`, of an LDAP user account with permissions to query the `basedn`. This command may be optional if your LDAP server does not require the FortiMail unit to authenticate when performing queries, and if you have enabled unauth-bind {enable | disable}.	
alias-bind-password <bindpw_str>	Enter the password of alias-bind-dn <bind_dn_str>	
alias-dereferencing {never | always | search | find}	Select the method to use, if any, when dereferencing attributes whose values are references: • `never`: Do not dereference. • `always`: Always dereference. • `search`: Dereference only when searching. • `find`: Dereference only when finding the base search object.	never
alias-expansion-level <limit_int>	Enter the maximum number of alias nesting levels that aliases the FortiMail unit will expand.	0
alias-group-expansion-state {enable | disable}	Enable if your LDAP schema resolves email aliases indirectly. For more information on direct vs. indirect resolution, see alias-bind-dn <bind_dn_str>.	disable

Variable	Description	Default
	When this option is **disabled**, alias resolution occurs using **one** query. The FortiMail unit queries the LDAP directory using the `basedn` and the `alias-member-query`, and then uses the value of each `alias-member-mail-attribute` to resolve the alias. When this option is **enabled**, alias resolution occurs using **two** queries: The FortiMail unit first performs a preliminary query using the `basedn` and `alias-group-query`, and uses the value of each `alias-group-member-attribute` as the base DN for the second query. The FortiMail unit performs a second query using the distinguished names from the preliminary query (instead of the `basedn`) and the `alias-member-query`, and then uses the value of each `alias-member-mail-attribute` to resolve the alias. The two-query approach is appropriate if, in your schema, alias objects are structured like group objects and contain references in the form of distinguished names of member user objects, rather than directly containing email addresses to which the alias resolves. In this case, the FortiMail unit must first “expand" the alias object into its constituent user objects before it can resolve the alias email address.	
alias-group-member-attribute <attribute_str>	Enter the name of the attribute for the group member, such as `member`, whose value is the DN of a user object. This attribute must be present in alias objects only if they do not contain an email address attribute specified in alias-member-mail-attribute <attribute_str>.	
alias-group-query <query_str>	Enter an LDAP query filter that selects a set of alias objects, represented as a group of member objects in the LDAP directory. The query filter string filters the result set, and should be based upon any attributes that are common to all alias objects but also exclude non-alias objects. For example, if alias objects in your directory have two distinguishing characteristics, their `objectClass` and `proxyAddresses` attributes, the query filter might be: `(&(objectClass=group) (proxyAddresses=smtp:$m))` where `$m` is the FortiMail variable for an email address.	

Variable	Description	Default
alias-member-mail-attribute <attribute_str>	Enter the name of the attribute for the alias member's mail address, such as `mail` or `rfc822MailMember`, whose value is an email address to which the email alias resolves, such as `user@example.com`. This attribute must be present in either alias or user objects, as determined by your schema and whether it resolves aliases directly or indirectly.	
alias-member-query <query_str>	Enter an LDAP query filter that selects a set of either user or email alias objects, whichever object class contains the attribute you configured in alias-member-mail-attribute <attribute_str>, from the LDAP directory. The query filter string filters the result set, and should be based upon any attributes that are common to all user/alias objects but also exclude objects that are not a user/alias. For example, if user objects in your directory have two distinguishing characteristics, their `objectClass` and `mail` attributes, the query filter might be: `(& (objectClass=alias) (mail=$m))` where `$m` is the FortiMail variable for a user's email address.	
alias-schema {activedirectory | dominoperson | inetlocalmailrcpt | inetorgperson | userdefined}	Enter either the name of the LDAP directory's schema, or enter `userdefined` to indicate a custom schema.	inetorgperson
alias-scope {base one | sub}	Enter which level of depth to query: • `base`: Query the `basedn` level. • `one`: Query only the one level directly below the `basedn` in the LDAP directory tree. • `sub`: Query recursively all levels below the `basedn` in the LDAP directory tree.	sub
alias-state {enable | disable}	Enable to query user objects for email address aliases.	disable
antispam <attribute_str>	Enter the name of the attribute, such as `antispam`, whose value indicates whether or not to perform antispam processing for that user.	
antivirus <attribute_str>	Enter the name of the attribute, such as `antivirus`, whose value indicates whether or not to perform antivirus processing for that user.	

Variable	Description	Default
asav-state {enable | disable}	Enable to query user objects for mappings between internal and external email addresses.	disable
auth-bind-dn {cnid | none | searchuser | upn}	Enter either none to not define a user authentication query, or one of the following to define a user authentication query: `cnid`: Enter the name of the user objects' common name attribute, such as `cn` or `uid`. `searchuser`: Enter to form the user's bind DN by using the DN retrieved for that user This command applies only if `schema` is `userdefined` in "set ldap_profile profile user" on page 2407. `upn`: Enter to form the user's bind DN by prepending the user name portion of the email address (`$u`) to the User Principle Name (UPN, such as `example.com`). By default, the FortiMail unit will use the mail domain as the UPN. If you want to use a UPN other than the mail domain, also configure upn-suffix <upns_str>.	searchuser
authstate {enable | disable}	Enable to perform user authentication queries.	disable
base-dn <base-dn_str>	Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail unit will search for user objects, such as `ou=People,dc=example,dc=com`. User objects should be child nodes of this location.	
bind-dn <bind-dn_str>	Enter the bind DN, such as `cn=FortiMailA,dc=example,dc=com`, of an LDAP user account with permissions to query the `basedn`. This command may be optional if your LDAP server does not require the FortiMail unit to authenticate when performing queries, and if you have enabled unauth-bind {enable | disable}.	
bind-password <bind-password_str>	Enter the password of bind-dn <bind-dn_str>.	
cache-state {enable | disable}	Enable to cache LDAP query results. Caching LDAP queries can introduce a delay between when you update LDAP directory information and when the FortiMail unit begins using that new information, but also has the benefit of reducing the amount of LDAP network traffic associated with frequent queries for information that does not change frequently.	disable

Variable	Description	Default
	If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of `0` effectively disables caching.	
cache-ttl <ttl_int>	Enter the amount of time, in minutes, that the FortiMail unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiMail unit to query the LDAP server, refreshing the cache. The default TTL value is 1,440 minutes (one day). The maximum value is 10,080 minutes (one week). Enter `0` to effectively disable caching.	1440
chain <ldap-profile_name>	Enter the LDAP profile that you want to add to the group of other LDAP profiles to create a chain query.	
chain-status {enable | disable}	Enable the chain query.	disable
client-cert-auth {enable | disable}	Enable if the LDAP server requires that clients such as the FortiMail unit present a client certificate to authenticate themselves during secure connections. Also configure client-cert <certificate_name>. This setting is only available when secure {none | ssl} is `ssl`.	disable
client-cert <certificate_name>	Enter the name of a local certificate if the LDAP server requires that clients such as the FortiMail unit present a client certificate to identify themselves during secure connections. FortiMail unit will use as its client certificate. This can be used instead of, or in addition to, a bind DN and password. Also configure client-cert-auth {enable | disable}. This setting is only available when secure {none | ssl} is `ssl`. **Note:** The certificate that FortiMail uses for client authentication must: • not be expired • not be revoked • be signed by a certificate authority (CA), whose certificate you have imported into the FortiMail unit and that the server trusts (directly or indirectly, proven via a signing chain) Otherwise the secure connection will fail. Servers may have their own certificate validation requirements in addition to FortiMail requirements. For example, client certificates may require that `Key Usage` field allow client authentication. See your LDAP server's documentation.	

Variable	Description	Default
cnid-name <cnid_str>	Enter the name of the user objects' common name attribute, such as `cn` or `uid`.	
content <content-profile_name>	Enter the name of the attribute, such as `genericContent`, whose value is the name of the content profile assigned to the domain. The name of this attribute may vary by the schema of your LDAP directory. If you do not specify this attribute (that is, leave this field blank), then the content profile in the matched recipient-based policy will be used.	
comment "<comment_str>"	Enter a description or comment.	
dereferencing {never | always | search | find}	Select the method to use, if any, when dereferencing attributes whose values are references. • `never`: Do not dereference. • `always`: Always dereference. • `search`: Dereference only when searching. • `find`: Dereference only when finding the base search object.	never
display-name <display-name_str>	Enter the LDAP address mapping display name attribute.	
domain-antispam-attr <attribute_str>	Enter the name of the antispam profile attribute, such as `businessCategory`, whose value is the name of the antispam profile assigned to the domain. The name of this attribute may vary by the schema of your LDAP directory.	
domain-antivirus-attr <attribute_str>	Enter the name of the antivirus profile attribute, such as `preferredLanguage`, whose value is the name of the antivirus profile assigned to the domain. The name of this attribute may vary by the schema of your LDAP directory.	
domain-content-attr <attribute_str>	Enter the content attribute name.	
domain-override {enable | disable}	Enable or disable override of the system admin domain.	
domain-override-attribute <attribute_str>	Enter the system admin domain override attribute.	

Variable	Description	Default
domain-parent-attr <attribute_str>	Enter the name of the parent domain attribute, such as `description`, whose value is the name of the parent domain from which a domain inherits the specific recipient check settings and quarantine report settings. The name of this attribute may vary by the schema of your LDAP directory.	
domain-query <query_str>	Enter an LDAP query filter that selects a set of domain objects, whichever object class contains the attribute you configured for this option, from the LDAP directory. For details on query syntax, refer to any standard LDAP query filter reference manual. For this option to work, your LDAP directory should contain a single generic user for each domain. Wildcard users (e.g. `*@$d`) are also supported for domain query, in cases where there is no generic domain user. The user entry should be configured with attributes to represent the following: • parent domain from which a domain inherits the specific RCPT check settings and quarantine report settings. For example, `description=parent.com` • IP address of the backend mail server hosting the mailboxes of the domain. For example, `mailHost=192.168.1.105` • antispam profile assigned to the domain. For example, `businessCategory=parentAntispam` • antivirus profile assigned to the domain. For example, `preferredLanguage=parentAntivirus`	
domain-routing-mail-host-attr <attribute_str>	Enter the name of the mail host attribute, such as `mailHost`, whose value is the name of the IP address of the backend mail server hosting the mailboxes of the domain. The name of this attribute may vary by the schema of your LDAP directory.	
domain-state {enable | disable}	Enable or disable the domain lookup option. For more information about domain lookup, see domain-query <query_str> on page 230.	disable
external-address <attribute_str>	Enter the name of the attribute whose value is an email address in the same or another protected domain.	extAddress

Variable	Description	Default
	This email address will be rewritten into the value of internal-address <attribute_str> according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings: on page 237. The name of this attribute may vary by the schema of your LDAP directory.	
fallback-port <port_int>	If you have configured a backup LDAP server that listens on a nonstandard port number, enter the TCP port number. The standard port number for LDAP is 389. The standard port number for SSL-secured LDAP is 636. The FortiMail unit will use SSL-secured LDAP to connect to the server if `secure` is `ssl`.	389
fallback-server {<server_fqdn> | <server_ipv4>}	Enter either the fully qualified domain name (FQDN) or IP address of the backup LDAP server. If there is no fallback server, enter an empty string ('').	
group-base-dn <base-dn_str>	Enter the base DN portion of the group's full DN, such as `ou=Groups,dc=example,dc=com`. This command applies only if `group-relative-name` is `enable`.	
group-expansion-level {1..6}	Enter how many levels of nested groups will be expanded for lookup. Valid range is 1-6.	1
group-membership-attribute <attribute_str>	Enter the name of the attribute, such as `memberOf` or `gidNumber`, whose value is the group number or DN of a group to which the user belongs. This attribute must be present in user objects. Whether the value must use common name, group number, or DN syntax varies by your LDAP server schema. For example, if your user objects use both `inetOrgPerson` and `posixAccount` schema, user objects have the attribute `gidNumber`, whose value must be an integer that is the group ID number, such as `10000`.	
group-name-attribute <attribute_str>	Enter the name of the attribute, such as `cn`, whose value is the group name of a group to which the user belongs. This command applies only if `group-relative-name` is `enable`.	

Variable	Description	Default
group-owner {enable | disable}	Enable to query the group object by its distinguished name (DN) to retrieve the DN of the group owner, which is a user that will receive that group's spam reports. Using that user's DN, the FortiMail unit will then perform a second query to retrieve that user's email address, where the spam report will be sent.For more information on sending spam reports to the group owner, see domain-setting on page 88.	disable
group-owner-address-attribute <attribute_str>	Enter the name of the attribute, such as `mail`, whose value is the group owner's email address. If `group-owner` is `enable`, this attribute must be present in user objects.	
group-owner-attribute <attribute_str>	Enter the name of the attribute, such as `groupOwner`, whose value is the distinguished name of a user object. You can configure the FortiMail unit to allow that user to be responsible for handling the group's spam report. If `group-owner` is `enable`, this attribute must be present in group objects.	
group-relative-name {enable | disable}	Enable to specify the base distinguished name (DN) portion of the group's full distinguished name (DN) in the LDAP profile. By specifying the group's base DN and the name of its group name attribute in the LDAP profile, you will only need to supply the group name value when configuring each feature that uses this query. For example, you might find it more convenient in each recipient-based policy to type only the group name, `admins`, rather than typing the full DN, `cn=admins,ou=Groups,dc=example,dc=com`. In this case, you could enable this option, then `basedn` (`ou=Groups,dc=example,dc=com`) and `groupnameattribute` (`cn`). When performing the query, the FortiMail unit would assemble the full DN by inserting the common name that you configured in the recipient-based policy between the `groupnameattribute` and the `basedn` configured in the LDAP profile. Note: Enabling this option is appropriate **only if** your LDAP server's schema specifies that the group membership attribute's value must use DN syntax. It is **not** appropriate if this value uses another type of syntax, such as a number or common name.	disable

Variable	Description	Default
	For example, if your user objects use both `inetOrgPerson` and `posixAccount` schema, user objects have the attribute `gidNumber`, whose value must be an integer that is the group ID number, such as `10000`. Because a group ID number does not use DN syntax, you would not enable this option.	
group-virtual {enable | disable}	Enable to use objects within the base DN of base-dn <base-dn_str> as if they were members of a user group object. For example, your LDAP directory might not contain user group objects. In that sense, groups do not really exist in the LDAP directory. However, you could mimic a group's presence by enabling this option to treat all users that are child objects of the base DN in the user object query as if they were members of such a group.	disable
groupstate {enable | disable}	Enable to perform LDAP group queries.	disable
internal-address <attribute_str>	Enter the name of the LDAP attribute whose value is an email address in the same or another protected domain. This email address will be rewritten into the value of external-address <attribute_str> according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings: on page 237. The name of this attribute may vary by the schema of your LDAP directory.	intAddress
port <port_int>	If you have configured a backup LDAP server that listens on a nonstandard port number, enter the TCP port number. The standard port number for LDAP is 389. The standard port number for SSL-secured LDAP is 636.	389
query <query_str>	Enter an LDAP query filter, enclosed in single quotes ('), that selects a set of user objects from the LDAP directory. The query filter string filters the result set, and should be based upon any attributes that are common to all user objects but also exclude non-user objects. For example, if user objects in your directory have two distinguishing characteristics, their `objectClass` and `mail` attributes, the query filter might be: `(& (objectClass=inetOrgPerson) (mail=$m))` where `$m` is the FortiMail variable for a user's email address.	(& (objectClass=inetOrgPerson) (mail=$m))

Variable	Description	Default

	If the email address (`$m`) as it appears in the message header is different from the user's email address as it appears in the LDAP directory, such as when you have enabled recipient tagging, a query for the user by the email address (`$m`) may fail. In this case, you can modify the query filter to subtract prepended or appended text from the user name portion of the email address before performing the LDAP query. For example, to subtract "-spam" from the **end** of the user name portion of the recipient email address, you could use the query filter:
	`(& (objectClass=inetOrgPerson) (mail=$m${-spam}))`
	where `${-spam}` is the FortiMail variable for the tag to remove before performing the query. Similarly, to subtract "spam-" from the **beginning** of the user name portion of the recipient email address, you could use the query filter:
	`(& (objectClass=inetOrgPerson) (mail=$m${^spam-}))`
	where `${^spam-}` is the FortiMail variable for the tag to remove before performing the query.
	For some schemas, such as Microsoft Active Directory-style schemas, this query will retrieve both the user's primary email address and the user's alias email addresses. If your schema style is different, you may want to also configure an alias query to resolve aliases.
	For details on query syntax, refer to any standard LDAP query filter reference manual.
	This command applies only if `schema` is `userdefined`.	

rcpt-vrfy-bypass {enable | disable}	If you have selected using LDAP server to verify recipient address and your LDAP server is down, enabling this option abandons recipient address verification and the FortiMail unit will continue relaying email.	enable
referrals-chase {enable | disable}	Enable chasing referrals.	disable
routing-mail-host <attribute_str>	Enter the name of the LDAP attribute, such as `mailHost`, whose value is the fully qualified domain name (FQDN) or IP address of the email server that stores email for the user's email account.	mailHost
routing-mail-addr <attribute_str>	Enter the name of the LDAP attribute whose value is the email address of a deliverable user on the email server, also known as the mail host.	mailRoutingAddress

Variable	Description	Default
	For example, a user may have many aliases and external email addresses that are not necessarily known to the email server. These addresses would all map to a real email account (mail routing address) on the email server (mail host) where the user's email is actually stored. A user's recipient email address located in the envelope or header portion of each email will be rewritten to this address.	
routing-state {enable | disable}	Enable to perform LDAP queries for mail routing.	disable
schema {activedirectory | dominoperson | inetlocalmailrcpt | inetorgperson | userdefined}	Enter either the name of the LDAP directory's schema, or enter `userdefined` to indicate a custom schema. If you enter `userdefined`, you must configure `query`.	inetorgperson
scope {base | one | sub}	Select which level of depth to query: • `base`: Query the `basedn` level. • `one`: Query only the one level directly below the `basedn` in the LDAP directory tree. • `sub`: Query recursively all levels below the `basedn` in the LDAP directory tree.	sub
secure {none | ssl}	Select whether or not to connect to the LDAP server (s) using an encrypted connection. • `none`: Use a non-secure connection. • `ssl`: Use an SSL/TLS-secured (LDAPS) connection. **Note:** If your FortiMail unit is deployed in server mode, and you want to enable webmail-password-change {enable | disable} using an LDAP server that uses a Microsoft Active Directory-style schema, then you must select `ssl`. Active Directory servers require a secure connection for queries that change user passwords.	none
server {<server_fqdn> | <server_ipv4> | <server_ipv6>	Enter the fully qualified domain name (FQDN) or IP address of the LDAP server.	
timeout <timeout_int>	Enter the maximum amount of time in seconds that the FortiMail unit will wait for query responses from the LDAP server.	10

Variable	Description	Default
unauth-bind {enable | disable}	An unauthenticated bind is a bind where the user supplies a user name with no password. Some LDAP servers (such as Active Directory) allow unauthenticated bind by default. For better security, FortiMail does not accept empty password when doing LDAP authentication even if the backend LDAP server allows it. In some cases, such as allowing all members of a distribution list to access their quarantined email in gateway and transparent mode, this option needs to be enabled in the LDAP profile, so that FortiMail can accept LDAP authentication requests with empty password (user name must not be empty), and forward such requests to the back-end LDAP server. If unauthenticated bind is permitted by the LDAP server, AND if the user exists on the server, FortiMail will consider authentication successful and grant access to the user. It is highly recommended that a dedicated LDAP profile (with this option enabled) is used for the above case. All other users should use separate LDAP profiles with this option disabled (this is the default setting) to maintain maximum security. ***Note***: This option is available in CLI only. And it only takes effect for webmail access in gateway and transparent mode.	disable
upn-suffix <upns_str>	If you want to use a UPN other than the mail domain, enter that UPN. This can be useful if users authenticate with a domain other than the mail server's principal domain name.	
user-display-name-attr <attribute_str>	Enter the name of the attribute that has the user's display name.	cn
user-display-name-retrieval {enable | disable}	Enable to retrieve the user's display name for webmail.	disable
version {ver2 | ver3}	Enter the version of the protocol used to communicate with the LDAP server.	ver3
webmail-password-change {enable | disable}	Enable to perform password change queries for FortiMail webmail users.	disable
webmail-password-schema {openldap | activedirectory}	Enter one of the following to indicate the schema of your LDAP directory: • `openldap`: The LDAP directory uses an OpenLDAP-style schema.	openldap

Variable	Description	Default
	• `activedirectory`: The LDAP directory uses a Microsoft Active Directory-style schema. **Note:** Microsoft Active Directory requires that password changes occur over an SSL/TLS-secured connection.	

Email address mapping

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

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

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

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

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

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

Match evaluation and rewrite behavior for email address mappings:

Order of evaluation	Match condition	If yes...	Rewrite to...
1	Does `RCPT TO:` match an **external** email address?	Replace `RCPT TO:`.	Internal email address

2	Does `MAIL FROM:` match an **internal** email address?	For each of the following, if it matches an internal email address, replace it:
		`MAIL FROM:`
		`RCPT TO:`
			External email address

Order of evaluation	Match condition	If yes...	Rewrite to...
		From: To: Return-Path: Cc: Reply-To: Return-Receipt-To: Resent-From: Resent-Sender: Delivery-Receipt-To: Disposition-Notification-To:	

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

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

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

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

Related topics

profile authentication
profile antispam
profile antivirus
profile ldap-mapping

profile ldap-mapping

Use this command to configure LDAP mapping profiles. These map LDAP attributes to the equivalent field of contacts in the FortiMail address book.

Before you configure the LDAP mapping, if required, on your LDAP server, configure the schema so that it works with a FortiMail LDAP profile query. For details, see the FortiMail Administration Guide. Also test the query results. If it contains data that you do not want to import into the address book, then you must configure filter <query-filter_str>.

To apply the LDAP attribute mapping, select it either while importing contacts on demand, or in a regularly scheduled address book synchronization.

This command is only available if either:

- in server mode
- in gateway and/or transparent mode, if `config mailsetting email-continuity` is configured

Syntax

```
config profile ldap-mapping
   edit <profile_name>
      [set comment "<comment_str>"]
      set filter <query-filter_str>
      config contact-attribute-mapping
         edit <mapping_int>
            set contact-attribute {email(WORK | display_name | ...}
            set ldap-attribute <attribute_str>
         next
      end
   next
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile.	
contact-attribute {email(WORK | display_name | ...}	Select an attribute in FortiMail webmail address book contacts (such as `display_name`) that you want to map to ldap-attribute <attribute_str>. **Note:** The `email(WORK)` attribute must be mapped because it identifies the entry in the address book. Other attributes may be required too, depending on which information you want to synchronize: • `display_name` • `first_name` • `last_name` • `nick_name` • `company` • `job_title` • `phonenumbers` • `phone(MOBILE)` • `addresses` • Any additional custom fields	
comment "<comment_str>"	Enter a description or comment.	
filter <query-filter_str>	If the query in the LDAP profile returns some results that you do not want to import into the address book, enter an LDAP query filter. For example, to select only results that have an email address, the filter might be:	

Variable	Description	Default
	`(mail=*)`	
ldap-attribute <attribute_str>	Select the name of the LDAP attribute on the directory server that corresponds to the contact-attribute {email(WORK | display_name | ...}. For example, the `cn` (common name) LDAP attribute might be mapped to `display_name`.	
<mapping_int>	Enter the number identifying the contact field that will be synchronized.	

Related topics

profile ldap

profile ldap-sync

profile ldap-sync

Use this command to configure synchronization with your directory server via LDAP. Synchronization can be regularly scheduled, or on demand.

Each contact is identified by its email address. If a new contact is created on the directory server, then synchronization adds it to the address book. If the same contact already exists in the address book, then synchronization updates it with current data from the directory server. If the contact does not exist on the directory server, then synchronization deletes that contact from the address book.

This command is only available if either:

- in server mode
- in gateway and/or transparent mode, if `config mailsetting email-continuity` is configured

Syntax

```
config profile ldap-sync
   edit <profile_name>
      [set description "<description_str>"]
      set status {enable | disable}
      set domain <protected-domain_name>
      set ldap-profile <profile_name>
      set mapping <profile_name>
      set sync-mode {full | incremental}
      set recurrence {daily | month | none | weekly}
      set schedule-hour {0..23}
      {set schedule-weekday {monday | tuesday | wednesday | thursday | friday | saturday |
            sunday}
       set schedule-date {1..31} }
```

```
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile.	
description "<description_str>"	Enter a description or comment.	
domain <protected-domain_name>	Select the protected domain whose address book you want to synchronize, or leave this setting empty to synchronize the global address book (`system`). **Note:** Once the LDAP synchronization task is created, this selection cannot be changed.	
ldap-profile <profile_name>	Select an LDAP profile that defines the base query and connection to the directory server.	
mapping <profile_name>	Select an LDAP attribute-to-address-book mapping that defines which contact information will be synchronized.	
recurrence {daily | month | none | weekly}	Select the time interval between each LDAP synchronization. If you select `none`, then you can use this profile to import the address book from the directory server at any time, on demand. For details, see the FortiMail Administration Guide. Otherwise, select when FortiMail automatically synchronizes: also configure schedule-hour {0..23}, schedule-weekday {monday | tuesday | wednesday | thursday | friday | saturday | sunday}, and schedule-date {1..31}.	none
schedule-date {1..31}	Enter the day of the month when LDAP synchronization will occur. This setting is available only when recurrence {daily | month | none | weekly} is `monthly`.	
schedule-hour {0..23}	Enter the hour of the day, according to a 24-hour clock, when LDAP synchronization will occur.	1
schedule-weekday {monday | tuesday | wednesday | thursday | friday | saturday | sunday}	Enter the day of the week when LDAP synchronization will occur. This setting is available only when recurrence {daily | month | none | weekly} is `weekly`.	
status {enable | disable}	Enable or disable this LDAP synchronization task.	enable
sync-mode {full | incremental}	Select how much to synchronize from the directory to the address book, either: • `full` — All data that matches the LDAP query and has an address book mapping. • `incremental` — Only data that changed since the most recent synchronization.	incremental

Variable	Description	Default
	For example, you might have both a daily incremental sync task (it's smaller, so it can run every night), and also a full sync task (it runs every weekend).	

Related topics

profile ldap
profile ldap-mapping

profile mail-routing

Use this command to configure email routing profiles, including MTA advanced control.

Syntax

```
config profile mail-routing
   edit <profile_name>
      config entry
         edit <id_entry>
            set recipient-pattern <string>
            set relay-to-host <string>
            set relay-to-port <integer>
            set relay-type {host | mx-lookup | mx-lookup-matched-domain | relay-host}
            set sender-pattern <string>
         next
      end
   next
end
```

Variable	Description	Default
recipient-pattern <string>	Enter the recipient pattern.	
relay-to-host <string>	Enter a pre-defined relay host.	
relay-to-port <integer>	Enter the SMTP port number.	25
relay-type {host | mx-lookup | mx-lookup-matched-domain | relay-host}	Set the relay type: • `host`: Relay matched session to specified SMTP server. • `mx-lookup`: Query the DNS server's MX record of a domain name you specify for the FQDN or IP address of the SMTP server. If there are multiple MX records, FortiMail will load balance between them.	host

Variable	Description	Default
	• `mx-lookup-match-domain`: Relay through the MX record lookup of the matched recipient domain. • `relay-host`: Relay to a pre-defined relay host.	
sender-pattern <string>	Enter the sender pattern.	

profile notification

Use this command configure a notification profile.

Note that domain users may only create one notification profile per domain.

Syntax

```
config profile notification
   edit <profile_name>
      set attach-original-message {enable | disable}
      set email-template <template_name>
      set other <recipient_address>
      set recipient {none | other | recipient | sender}
      set type {generic | sender_addr_rate_ctrl}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the notification profile.	
attach-original-message {enable | disable}	Enable to include the original message as attachment in the notification email.	disable
email-template <template_name>	Specify the email template to use.	default
other <recipient_address>	Specify the recipient address for the notification email.	
recipient {none | other | recipient | sender}	Specify who you want to send the notification to.	none
type {generic | sender_addr_rate_ctrl}	Specify the type of notification profile.	generic

profile replacement-message

Use this command to configure custom replacement messages for the subject, body, or attachments to be used for content and DLP scanning.

Syntax

```
config profile replacement-message
   edit <name>
      config member
         edit ...
            set content <string>
            set comment <string>
         next
      end
      set comment
   next
end
```

Variable	Description	Default
edit ...	Configure the various email replacement message types: • content-subject • content-body • content-attachment-blocked • content-attachment-number-limit-exceeded • content-attachment-size-limit-exceeded • content-size-limit-exceeded • dlp-subject • dlp-body • dlp-attachment • virus-body • virus-attachment-infected • virus-attachment-suspicious	
content <string>	Enter the content of the specific replacement message. Note there is a 8191 character limit for each replacement message.	

Related topics

customized-message

profile resource

Use this command configure a resource profile.

This command only applies in the server mode.

Syntax

```
config profile resource
   edit <profile_name>
      set auto-check-message {enable | disable}
      set auto-delete-old-mail <days>
      set auto-delete-sent-folder <days>
      set auto-delete-trash-folder <days>
      set auto-forward {enable | disable}
      set auto-reply {enable | disable}
      set email-continuity-status {enable | disable}
      set idle-timeout {enable | disable}
      set message-filter {enable | disable}
      set mobile-access {enable | disable}
      set outbound-safelist
      set quarantine-bcc-addr
      set quarantine-bcc-status
      set quarantine-days
      set quarantine-report {enable | disable}
      set quota <MB_int>
      set release-auto-safelist {enable | disable}
      set release-through-email {enable | disable}
      set release-through-web {enable | disable}
      set status {enable | disable}
      set webmail-access {enable | disable}
      set webmail-addressbook-access {domain | none | system}
      set webmail-user-preference {enable | disable}
end
```

Variable	Description	Default
auto-check-message {enable | disable}	Enable or disable auto checking for new messages in FortiMail webmail.	enable
<profile_name>	Enter the name of the notification profile.	
auto-delete-old-mail <days>	Enter the number of days after which the FortiMail unit will automatically delete email that is locally hosted. 0 means not to delete email.	0
auto-delete-sent-folder <days>	Enter the number of days after which the FortiMail unit will automatically delete email in the sent folder. 0 means not to delete email.	0

Variable	Description	Default
auto-delete-trash-folder <days>	Enter the number of days after which the FortiMail unit will automatically empty the trash folder. 0 means not to delete email.	14
auto-forward {enable | disable}	Enable to allow auto forward in webmail.	enable
auto-reply {enable | disable}	Enable to allow auto reply in webmail.	enable
email-continuity-status {enable | disable}	Enable or disable email continuity. When the SMTP server is detected as inaccessible, recipient verification is skipped and emails are put into the email continuity queue. When the SMTP server is accessible again, the email is delivered. This feature requires a valid feature license. **Note:** There is no DSN if the email is from an unknown user.	enable
idle-timeout {enable | disable}	Enable to enforce an idle timeout on webmail sessions. See also webmail-session-ttl <seconds_int>.	enable
message-filter {enable | disable}	Enable to allow message filtering in webmail.	enable
mobile-access {enable | disable}	Enable to allow mobile users to access their email via webmail.	enable
outbound-safelist	Enable or disable automatically updating personal safelists from sent emails.	disable
quarantine-bcc-addr	Enter the comma separated email address of BCC.	
quarantine-bcc-status	Enable or disable BCC messages to specified emails when quarantined emails released.	disable
quarantine-days	Enter the number of days a quarantined message is kept. Enter 0 for indefinitely.	14
quarantine-report {enable | disable}	Enable or disable the generation of summary reports of the quarantined emails.	enable
quota <MB_int>	Enter the user's disk space quota in megabytes.	1000
release-auto-safelist {enable | disable}	Automatically add sender of a released message to personal safelist.	enable
release-through-email {enable | disable}	Enable or disable auto release quarantined emails through email	disable
release-through-web {enable | disable}	Enable or disable auto release quarantined emails through the web.	enable

Variable	Description	Default
status {enable | disable}	Enable or disable the user account.	enable
webmail-access {enable | disable}	Enable or disable user's webmail access.	enable
webmail-addressbook-access {domain | none | system}	Enable or disable user access to system and/or domain address book.	
webmail-user-preference {enable | disable}	Enable or disable the user preferences for FortiMail webmail.	enable

profile session

Use this command to create session profiles.

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

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

Syntax

```
config profile session
   edit <profile_name>
      set access-control <profile_name>
      set block-encrypted {enable | disable}
      set bypass-bounce-verification {enable | disable}
      set check-client-ip-quick {enable | disable}
      set conn-blocklisted {enable | disable}
      set conn-concurrent <connections_int>
      set conn-hidden {enable | disable}
      set conn-idle-timeout <timeout_int>
      set conn-total <connections_int>
      set dkim-signing {enable | disable}
      set dkim-signing-authenticated-only {enable | disable}
      set dkim-validation {enable | disable}
      set domain-key-validation {enable | disable}
      set email-addr-rewrite-options {envelope-from | envelope-from-as-key | envelope-to |
            header-from | header-to | reply-to}
      set email-queue {default | incoming | no-preference | outgoing}
      set endpoint-reputation {enable | disable}
      set endpoint-reputation-action {reject | monitor}
      set endpoint-reputation-blocklist-duration <duration_int>
      set endpoint-reputation-blocklist-trigger <trigger_int>
```

```
        set eom-ack {enable | disable}
        set error-drop-after <errors_int>
        set error-penalty-increment <penalty-increment_int>
        set error-penalty-initial <penalty-initial_int>
        set error-penalty-threshold <threshold_int>
        set fortiguard-ip-check-mode {as-profile | as-profile-no-auth | client-connect | disable}
        set limit-NOOPs <limit_int>
        set limit-RSETs <limit_int>
        set limit-email <limit_int>
        set limit-helo <limit_int>
        set limit-max-header-size <limit_int>
        set limit-max-message-size <limit_int>
        set limit-recipient <limit_int>
        set mail-route <profile_name>
        set number-of-messages <limit_int>
        set number-of-recipients <limit_int>
        set recipient-blocklist-status {enable | disable}
        set recipient-rewrite-map <profile_name>
        set recipient-safelist-status {enable | disable}
        set remote-log <profile_name>
        set remove-current-headers {enable | disable}
        set remove-headers {enable | disable}
        set remove-received-headers {enable | disable}
        set sender-blocklist-status {enable | disable}
        set sender-reputation-reject-score <threshold_int>
        set sender-reputation-status {enable | disable}
        set sender-reputation-tempfail-score <threshold_int>
        set sender-reputation-throttle-number <rate_int>
        set sender-reputation-throttle-percentage <percentage_int>
        set sender-reputation-throttle-score <threshold_int>
        set sender-rewrite-map <profile_name>
        set sender-safelist-status {enable | disable}
        set sender-verification {enable | disable}
        set sender-verification-profile <profile_name>
        set session-3way-check {enable | disable}
        set session-action <content-action_profile>
        set session-action-msg-type {accepted | all}
        set session-allow-pipelining {yes | no}
        set session-command-checking {enable | disable}
        set session-disallow-encrypted {enable | disable}
        set session-helo-char-validation {enable | disable}
        set session-helo-domain-check {enable | disable}
        set session-helo-rewrite-clientip {enable | disable}
        set session-helo-rewrite-custom {enable | disable}
        set session-helo-rewrite-custom-string <helo_str>
        set session-prevent-open-relay {enable | disable}
        set session-recipient-domain-check {enable | disable}
        set session-reject-empty-domain {enable | disable}
        set session-sender-domain-check {enable | disable}
        set spf-validation {enable | disable}
        set splice-status {enable | disable}
        set splice-threshold <threshold_int>
        set splice-unit {seconds | kilobytes}
        config header-removal-list
           edit <header-key_str>
           next
        config recipient-blocklist
```

```
            edit <block-recipient-address_str>
            next
        config recipient-safelist
            edit <safe-recipient-address_str>
            next
        config sender-blocklist
            edit <block-sender-address_str>
            next
        config sender-safelist
            edit <safe-sender-address_str>
            next
        end
    next
end
```

Variable	Description	Default
<profile_name>	Enter the name of the session profile.	
<header-key_str>	Enter a message header key such as `X-Custom` to remove that header from email messages. This setting applies only if remove-headers {enable | disable} on page 254 is enabled.	
<block-recipient-address_str>	Enter a blocklisted recipient email address. This setting applies only if recipient-blocklist-status {enable | disable} on page 254 is enabled.	
<safe-recipient-address_str>	Enter a safelisted recipient email address. This setting applies only if recipient-safelist-status {enable | disable} on page 254 is enabled.	
<block-sender-address_str>	Enter a blocklisted sender email address. This setting applies only if sender-blocklist-status {enable | disable} on page 255 is enabled.	
<safe-sender-address_str>	Enter a safelisted sender email address. This setting applies only if sender-safelist-status {enable | disable} on page 256 is enabled.	
access-control <profile_name>	Enter an access control profile to be used in a session profile. **Note:** This feature is only available as part of the MTA advanced control feature. See mta-adv-ctrl-status {enable | disable} on page 313	
block-encrypted {enable | disable}	Enable or disable blocking of TLS/MD5 commands so that email must pass unencrypted. Email must not be encrypted in order for the FortiMail unit to scan the email for viruses and spam. This option applies only if the FortiMail unit is operating in transparent mode.	disable
bypass-bounce-verification {enable | disable}	Select to, if bounce verification is enabled, omit verification of bounce address tags on incoming bounce messages. This bypass does not omit bounce address tagging of outgoing email.	disable

Variable	Description	Default
	Alternatively, you can omit bounce verification with a per-domain setting. See bypass-bounce-verification {enable | disable} on page 90. For information on enabling bounce address tagging and verification (BATV), see antispam bounce-verification on page 43.	
check-client-ip-quick {enable | disable}	Enable to query the FortiGuard Antispam Service to determine if the IP address of the SMTP server is blocklisted. This action will happen during the connection phase. In an antispam profile, you can also enable FortiGuard block-IP checking. But that action happens after the entire message has been received by FortiMail. Therefore, if this feature is enabled in a session profile and the action is reject, the performance will be improved.	disable
conn-blocklisted {enable | disable}	Enable to prevent clients from using SMTP servers that have been blocklisted in antispam profiles or, if enabled, the FortiGuard AntiSpam service. This option applies only if the FortiMail unit is operating in transparent mode.	disable
conn-concurrent <connections_int>	Enter a limit to the number of concurrent connections per SMTP client. Additional connections are rejected. To disable the limit, enter `0`.	0
conn-hidden {enable | disable}	Select either: • `enable`: Be transparent. Preserve the IP address or domain name in: the SMTP greeting (`HELO`/`EHLO`) in the envelope, the `Received:` message headers of email messages, and the IP addresses in the IP header source and destination. This masks the existence of the FortiMail unit to the protected SMTP server. • `disable`: Do not be transparent. Replace the SMTP client's IP addresses or domain names with that of the FortiMail unit. This option applies only if the FortiMail unit is operating in transparent mode. For more information about the proxies and built-in MTA transparency, see the FortiMail Administration Guide. **Note:** Unless you have enabled exclusive {enable | disable}, the per-domain hide option (tp-hidden {no | yes}) has precedence over this option, and may prevent it from applying to incoming email messages. **Note:** For full transparency, also set the per-domain hide option (tp-hidden {no | yes}) to `yes`.	disable
conn-idle-timeout <timeout_int>	Enter a limit to the number of seconds a client may be inactive before the FortiMail unit drops the connection. Set the value between 5-1200.	30
conn-rate-number <connections_int>	This is a rate limit to the number of messages sent per client IP address per time interval (the default value is 30 minutes). You set the time interval using the command: `config antispam settings`	0

Variable	Description	Default

	`set session-profile-rate-control-interval <minutes>`
	`end`
	To disable the limit, enter `0`.	

conn-total <connections_int>	Enter a limit to the total number of concurrent connections from all sources. To disable the limit, enter `0`.	0
dkim-signing {enable | disable}	Enable to sign outgoing email with a DKIM signature. This option requires that you first generate a domain key pair and publish the public key in the DNS record for the domain name of the protected domain. If you do not publish the public key, destination SMTP servers will not be able to validate your DKIM signature. For details on generating domain key pairs and publishing the public key, see the FortiMail Administration Guide.	disable
dkim-signing-authenticated-only {enable | disable}	Enable to sign outgoing email with a DKIM signature only if the sender is authenticated. This option is available only if `dkim-signing` is `enable`.	disable
dkim-validation {enable | disable}	Enable to, if a DKIM signature is present, query the DNS server that hosts the DNS record for the sender's domain name to retrieve its public key to decrypt and verify the DKIM signature. An invalid signature increases the client sender reputation score and affect the deep header scan. A valid signature decreases the client sender reputation score. If the sender domain DNS record does not include DKIM information or the message is not signed, the FortiMail unit omits the DKIM signature validation.	disable
domain-key-validation {enable | disable}	Enable if the DNS record for the domain name of the sender lists DomainKeys. An unauthorized client IP address increases the client sender reputation score. An authorized client IP address decreases the client sender reputation score. If the DNS record for the domain name of the sender does not publish DomainKeys information, the FortiMail unit omits the DomainKeys client IP address validation.	disable
email-addr-rewrite-options {envelope-from | envelope-from-as-key | envelope-to | header-from | header-to | reply-to}	Specify which elements of the sender and recipient addresses to rewrite. For more details, see the session profile section in the FortiMail Administration Guide.	

Variable	Description	Default
email-queue {default | incoming | no-preference | outgoing}	Enter the email queue to use for the matching sessions. **Note:** This feature is only available as part of the MTA advanced control feature. See mta-adv-ctrl-status {enable | disable} on page 313	no-preference
endpoint-reputation {enable | disable}	Enable to accept, monitor, or reject email based upon endpoint reputation scores. This option is designed for use with SMTP clients with dynamic IP addresses. It requires that your RADIUS server provide mappings between dynamic IP addresses and MSISDNs/subscriber IDs to the FortiMail unit. If this profile governs sessions of SMTP clients with static IP addresses, instead consider sender-reputation-status {enable | disable} on page 255.	disable
endpoint-reputation-action {reject | monitor}	Select either: • `reject`: Reject email and MMS messages from MSISDNs/subscriber IDs whose MSISDN reputation scores exceed ***Auto blocklist score trigger value***. • `monitor`: Log, but do not reject, email and MMS messages from MSISDNs/subscriber IDs whose MSISDN reputation scores exceed `endpoint-reputation-blocklist-trigger <trigger_int> on page 252`. Log entries appear in the history log.	reject
endpoint-reputation-blocklist-duration <duration_int>	Enter the number of minutes that an MSISDN/subscriber ID will be prevented from sending email or MMS messages after they have been automatically blocklisted.	0
endpoint-reputation-blocklist-trigger <trigger_int>	Enter the MSISDN reputation score over which the FortiMail unit will add the MSISDN/subscriber ID to the automatic blocklist. The trigger score is relative to the period of time configured as the automatic blocklist window.	5
eom-ack {enable | disable}	Enable to acknowledge the end of message (`EOM`) signal immediately after receiving the carriage return and line feed (`CRLF`) characters that indicate the `EOM`, rather than waiting for antispam scanning to complete. If the FortiMail unit has not yet completed antispam scanning by the time that four (4) minutes has elapsed, it will return SMTP reply code 451(`Try again later`), resulting in no permanent problems, as according to RFC 2281, the minimum timeout value should be 10 minutes. However, in rare cases where the server or client's timeout is shorter than 4 minutes, the sending client or server could time-out while waiting for the FortiMail unit to acknowledge the `EOM` command. Enabling this option prevents those rare cases.	disable
error-drop-after <errors_int>	Enter the total number of errors the FortiMail unit will accept before dropping the connection.	5

Variable	Description	Default
error-penalty-increment <penalty-increment_int>	Enter the number of seconds by which to increase the delay for each error after the first delay is imposed.	1
error-penalty-initial <penalty-initial_int>	Enter the delay penalty in seconds for the first error after the number of “free" errors is reached.	1
error-penalty-threshold <threshold_int>	Enter the number of number of errors permitted before the FortiMail unit will penalize the SMTP client by imposing a delay.	1
fortiguard-ip-check-mode {as-profile | as-profile-no-auth | client-connect | disable}	Specify the FortiGuard IP reputation check mode: • `as-profile`: Uses the settings of the FortiGuard IP reputation in the antispam profile. • `as-profile-no-auth`: Uses the settings of the FortiGuard IP reputation in the antispam profile, but disable SMTP authentication when the client IP reputation score triggers the threshold. • `client-connect`: Checks FortiGuard IP reputation the moment a client connects. • `disable`: Disables FortiGuard IP reputation check.	as-profile
limit-NOOPs <limit_int>	Enter the limit of `NOOP` commands that are permitted per SMTP session. Some spammers use `NOOP` commands to keep a long session alive. Legitimate sessions usually require few `NOOP`s. Enter 0 to reset to the default value.	10
limit-RSETs <limit_int>	Enter the limit of `RSET` commands that are permitted per SMTP session. Some spammers use `RSET` commands to try again after receiving error messages such as unknown recipient. Legitimate sessions should require few `RSET`s. To disable the limit, enter `0`.	20
limit-email <limit_int>	Enter the limit of email messages per session to prevent mass mailing. To disable the limit, enter `0`.	10
limit-helo <limit_int>	Enter the limit of SMTP greetings that a connecting SMTP server or client can perform before the FortiMail unit terminates the connection. Restricting the number of SMTP greetings allowed per session makes it more difficult for spammers to probe the email server for vulnerabilities, as a greater number of attempts results in a greater number of terminated connections, which must then be re-initiated. Enter 0 to reset to the default value.	3
limit-max-header-size <limit_int>	Enter the limit of the message header size. If enabled, messages with headers over the threshold size are rejected.	32

Variable	Description	Default
limit-max-message-size <limit_int>	Enter the limit of message size in kilobytes (KB) . If enabled, messages over the threshold size are rejected. **Note:** If both this option and max-message-size <limit_int> in the protected domain are enabled, email size will be limited to whichever size is smaller.	10240
limit-recipient <limit_int>	Enter the limit of recipients to prevent mass mailing.	500
mail-route <profile_name>	Enter a mail routing profile to be used in a session profile.	
number-of-messages <limit_int>	Enter the number of message per client per time interval. To disable the limit, enter `0`. To set the time interval, see session-profile-rate-control-interval <minutes_int> on page 59.	30
number-of-recipients <limit_int>	Enter the number of recipients per client per time interval. To disable the limit, enter `0`. Then set the time interval using session-profile-rate-control-interval <minutes_int> on page 59.	30
recipient-blocklist-status {enable | disable}	Enable to use an envelope recipient (`RCPT TO:`) blocklist in SMTP sessions to which this profile is applied, then define blocklisted email addresses using <block-recipient-address_str>.	disable
recipient-rewrite-map <profile_name>	Enter an address rewrite profile to be used in a session profile. **Note:** This feature is only available as part of the MTA advanced control feature. See mta-adv-ctrl-status {enable | disable} on page 313	
recipient-safelist-status {enable | disable}	Enable to use an envelope recipient (`RCPT TO:`) safelist in SMTP sessions to which this profile is applied, then define safelisted email addresses using <safe-recipient-address_str>.	disable
remote-log <profile_name>	Enter the name of a remote logging profile.The remote logging profiles used here are the same as the system-wide remote logging profiles. **Note:** This feature is only available as part of the MTA advanced control feature. See mta-adv-ctrl-status {enable | disable} on page 313	
remove-current-headers {enable | disable}	Enable to remove the headers that are inserted by this FortiMail unit, except `DKIM-Signature:`. **Note**: For backwards compatibility, if you upgrade the firmware and both of the related settings remove-headers {enable | disable} on page 254 and remove-received-headers {enable | disable} on page 255 were enabled, then this setting will be enabled by default.	enable
remove-headers {enable | disable}	Enable to remove other configured headers from email messages. Enable to remove other headers that have been inserted by other MTAs (not this FortiMail), then configure which headers should be removed in <header-key_str> on page 249.	disable

Variable	Description	Default
remove-received-headers {enable | disable}	Enable to remove all `Received:` message headers that have been inserted by other MTAs (not this FortiMail). Alternatively, you can remove this header with a per-domain setting. For details, see remove-outgoing-received-header {enable | disable} on page 98.	disable
sender-blocklist-status {enable | disable}	Enable to use an envelope sender (`MAIL FROM:`) blocklist in SMTP sessions to which this profile is applied, then define the blocklisted email addresses using <block-sender-address_str>.	disable
sender-reputation-reject-score <threshold_int>	Enter a sender reputation score over which the FortiMail unit will return a rejection error code when the SMTP client attempts to initiate a connection. This option applies only if sender-reputation-status {enable | disable} is enabled.	80
sender-reputation-status {enable | disable}	Enable to reject email based upon sender reputation scores.	disable
sender-reputation-tempfail-score <threshold_int>	Enter a sender reputation score over which the FortiMail unit will return a temporary failure error code when the SMTP attempts to initiate a connection. This option applies only if sender-reputation-status {enable | disable} is enabled.	55
sender-reputation-throttle-number <rate_int>	Enter the maximum number of email messages per hour that the FortiMail unit will accept from a throttled SMTP client.	5
sender-reputation-throttle-percentage <percentage_int>	Enter the maximum number of email messages per hour that the FortiMail unit will accept from a throttled SMTP client, as a percentage of the number of email messages that the sender sent during the previous hour.	1
sender-reputation-throttle-score <threshold_int>	Enter the sender reputation score over which the FortiMail unit will rate limit the number of email messages that can be sent by this SMTP client. The enforced rate limit is either sender-reputation-throttle-number <rate_int> or sender-reputation-throttle-percentage <percentage_int> whichever value is greater. This setting applies only if sender-reputation-status {enable | disable} is enabled.	15
sender-rewrite-map <profile_name>	Enter an address rewrite profile to be used in a session profile. **Note:** This feature is only available as part of the MTA advanced control feature. See mta-adv-ctrl-status {enable | disable} on page 313	

Variable	Description	Default
sender-safelist-status {enable | disable}	Enable to use an envelope sender (`MAIL FROM:`) safelist in SMTP sessions to which this profile is applied, then define safelisted email addresses using <safe-sender-address_str>.	disable
sender-verification {enable | disable}	Enable sender address verification with LDAP.	disable
sender-verification-profile <profile_name>	Select the LDAP profile to use for sender address verification.	
session-3way-check {enable | disable}	Enable to reject the email if the domain name in the SMTP greeting (`HELO`/`EHLO`) and recipient email address (`RCPT TO:`) match, but the domain name in the sender email address (`MAIL FROM:`) does not. Mismatching domain names is sometimes used by spammers to mask the true identity of their SMTP client. This check only affects unauthenticated sessions.	disable
session-action <content-action_profile>	Select a content action profile to apply upon session policy match.	
session-action-msg-type {accepted | all}	Define the message type to take session action.	all
session-allow-pipelining {yes | no}	Select the behavior for ESMTP command pipelining: • `yes`: Accept some SMTP commands to be given and processed as a batch, increasing performance over high-latency connections. • `no`: Accept only one command at a time during an SMTP session. Do not accept the next command until it completes processing of the previous command. Pipelining may also occur implicitly, even if an email server or FortiMail does not explicitly say that it supports pipelining. See smtp-eom-bare-lf-handling {allow | disallow | ignore} on page 335.	yes

session-command-checking {enable | disable}	Enable to return SMTP reply code 503, rejecting the SMTP command, if the client or server uses SMTP commands that are syntactically incorrect.
	`EHLO` or `HELO`, `MAIL FROM:`, `RCPT TO:` (can be multiple), and `DATA` commands must be in that order. `AUTH`, `STARTTLS`, `RSET`, `NOOP` commands can arrive at any time. Other commands, or commands in an unacceptable order, return a syntax error.
	In the following example, the invalid commands are highlighted in bold:
	`220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:41:15 GMT`
	`EHLO example.com`
	`250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you`
		disable

Variable	Description	Default
	RCPT TO:<user1@example.com> 503 5.0.0 Need MAIL before RCPT	
session-disallow-encrypted {enable | disable}	Enable to block TLS/MD5 commands so that email must pass unencrypted, enabling the FortiMail unit to scan the email for viruses and spam. Clear to pass TLS/MD5 commands, allowing encrypted email to pass. The FortiMail unit cannot scan encrypted email for viruses and spam. This option applies only if the FortiMail unit is operating in transparent mode.	disable
session-helo-char-validation {enable | disable}	Enable to return SMTP reply code 501, rejecting the SMTP greeting, if the client or server uses a greeting that contains a domain name with invalid characters. To avoid disclosure of a real domain name, spammers sometimes spoof an SMTP greeting domain name with random characters, rather than using a genuine, valid domain name. If this option is enabled, such connections are rejected. In the following example, the invalid command is highlighted in bold: 220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:30:20 GMT ***EHLO ^^&^&^#$*** 501 5.0.0 Invalid domain name Valid characters for domain names include: • alphanumerics (A to Z and 0 to 9) • brackets ([and]) • periods (.) • dashes (-) • underscores (_) • number symbols(#) • colons (:)	disable
session-helo-domain-check {enable | disable}	Enable to return SMTP reply code 501, rejecting the SMTP greeting, if the client or server uses a greeting that contains a domain name with invalid characters. To avoid disclosure of a real domain name, spammers sometimes spoof an SMTP greeting domain name with random characters, rather than using a genuine, valid domain name. If this option is enabled, such connections are rejected. In the following example, the invalid command is highlighted in bold: 220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:30:20 GMT **EHLO ^^&^&^#$** 501 5.0.0 Invalid domain name Valid domain characters include: • alphanumerics (A to Z and 0 to 9) • brackets ([and]) • periods (.)	disable

Variable	Description	Default
	• dashes (-) • underscores (_) • number symbols(#) • colons (:)	
session-helo-rewrite-clientip {enable | disable}	Enable to rewrite the HELO/EHLO domain to the IP address of the SMTP client to prevent domain name spoofing. This option applies only if the FortiMail unit is operating in transparent mode.	disable
session-helo-rewrite-custom {enable | disable}	Enable to rewrite the HELO/EHLO domain, then enter the replacement text using session-helo-rewrite-custom-string <helo_str>. This option applies only if the FortiMail unit is operating in transparent mode.	disable
session-helo-rewrite-custom-string <helo_str>	Enter the replacement text for the HELO/EHLO domain.	
session-prevent-open-relay {enable | disable}	Enable to block unauthenticated outgoing connections to unprotected mail servers in order to prevent clients from using open relays to send email. If clients from your protected domains are permitted to use open relays to send email, email from your domain could be blocklisted by other SMTP servers. This feature: • applies only if the FortiMail unit is operating in transparent mode, • only affects unauthenticated sessions, and • is applicable only if you allow clients to use an unprotected SMTP server for outgoing connections. For details, see mailsetting proxy-smtp on page 128.	disable

session-recipient-domain-check {enable | disable}	Enable to return SMTP reply code 550, rejecting the SMTP command, if the domain name portion of the recipient address is not a domain name that exists in either MX or A records.
	In the following example, the invalid command is highlighted in bold:
	`220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 14:48:32 GMT`
	`EHLO example.com`
	`250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you`
	`MAIL FROM:<user1@fortinet.com>`
	`250 2.1.0 <user1@fortinet.com>... Sender ok`
	`RCPT TO:<user2@example.com>`
	`550 5.7.1 <user2@example.com>... Relaying denied. IP name lookup failed [192.168.1.1]`
	This check only affects unauthenticated sessions.
		disable

session-reject-empty-domain {enable | disable}	Enable to return SMTP reply code 553, rejecting the SMTP command, if a domain name does not follow the “@" symbol in the sender email address. Because the sender address is invalid and therefore cannot receive delivery status notifications (DSN), you may want to disable this feature.	disable

Variable	Description	Default

	In the following example, the invalid command is highlighted in bold:
	`220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2007 14:48:32 GMT`
	`EHLO example.com`
	`250-FortiMail-400.localdomain Hello [192.168.171.217], pleased to meet you`
	`MAIL FROM:<john@>`
	`553 5.1.3 <john@>... Hostname required`
	This check only affects unauthenticated sessions.	

session-sender-domain-check {enable | disable}	Enable o return SMTP reply code 421, rejecting the SMTP command, if the domain name portion of the sender address is not a domain name that exists in either MX or A records.
	In the following example, the invalid command is highlighted in bold:
	`220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 14:32:51 GMT`
	`EHLO`
	`250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you`
	`MAIL FROM:<user1@example.com>`
	`421 4.3.0 Could not resolve sender domain.`
		disable

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

Related topics

profile encryption

profile sso

Use this command to configure connections with remote authentication servers such as FortiAuthenticator that support single sign-on (SSO) protocols.

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

- FortiMail, which is the service provider (SP). See system saml on page 340.
- FortiAuthenticator or other remote authentication server, which is the identity provider (IdP)

To do this, you must:

1. On the IdP server:
   a. Download its IdP metadata XML.
      Alternatively, copy the URL where FortiMail can download it.
   b. The email address that the user must give when they authenticate is stored in an attribute on the IdP server. This attribute has an object identifier (OID). If this OID is different than the default setting of remote-user-attribute-name "<attribute_str>" on FortiMail, then copy the IdP server's OID. For example:
   c. `urn:oid:0.9.2342.19200300.100.1.3`
2. On FortiMail:
   a. If you are integrating with FortiAuthenticator or Ping Identity, then on FortiMail, use the CLI to enable Security Fabric and the administrator account named `admin_sso`:

      ```
      config system csf
         set status enable
      end
      config system admin
         edit admin_sso
            set status enable
      end
      ```

      The `admin_sso` account acts as a wildcard, so that you do not need to configure all FortiMail accounts on the IdP too. The Security Fabric provides communication for this feature.
   b. Paste the IdP metadata XML into an SSO profile. If the IdP uses a different attribute OID than the FortiMail default, then also configure that.
      See idp-metadata <idp-xml_str> and remote-user-attribute-name "<attribute_str>".
      Now FortiMail automatically generates its SP metadata, entity ID, and ACS URL. (You might need to navigate away from the tab and return in order for it to display.)
   c. Enable SSO. Copy the SP entity ID, ACS URL, and metadata XML.
      See system saml on page 340.
3. On the IdP server:

   a. Paste the entity ID, SP metadata URL, and ACS URL from FortiMail.
   b. Select to identify users by their email addresses attribute, and then enter the attribute object identifier (OID) that authentication requests from FortiMail use:

      `urn:oid:0.9.2342.19200300.100.1.3`
   c. Optionally, enable and configure multi-factor authentication (MFA).
   d. If required, add the FortiMail unit's certificate to the list of trusted CAs ("trust store").

      (Skip this step if your IdP already trusts the certificate, directly or indirectly, via a CA certificate signing chain.)
4. On FortiMail, for each account that will use SAML SSO to log in, configure:
   - auth-strategy {cloud | ldap | local | pki | radius | sso} and sso-profile <profile_name> (administrator accounts)
   - sso-status {enable | disable} and sso-profile <profile_name> (protected domain users)

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

Syntax

```
config profile sso
   edit <profile_name>
      set comment <description_str>
      set remote-user-attribute-name "<attribute_str>"
      set idp-metadata <idp-xml_str>
end
```

Variable	Description	Default
<profile_name>	Enter a unique name for the profile.	
comment <description_str>	Enter a descriptive comment.	
idp-metadata <idp-xml_str>	Enter the XML metadata that contains the X.509 server certificate, supported protocols, and service URLs of the identity provider (IdP).	
remote-user-attribute-name "<attribute_str>"	Enter the object identifier (OID) of email addresses on the IdP server. If you do not enter an OID, then FortiMail uses the default OID `urn:oid:0.9.2342.19200300.100.1.3`.	

Related topics

domain

system admin

system appearance

system saml

profile tls

Use this command to configure TLS profiles that can be used by policy access-control receive and policy access-control delivery.

Note: Many subcommands are only available when `level` is set to either `preferred` or `secure`.

Syntax

```
config profile tls
   edit <profile_name>
      set level {none | preferred | secure}
      set action {fail | tempfail}
      set ca-name <ca_name>
      set cert-subject <subject_str>
      set check-ca-name {enable | disable}
      set check-ca-type {match | substring | wildcard}
      set check-cert-subject {enable | disable}
      set check-cert-type {match | substring | wildcard}
      set check-encryption-strength {enable | disable}
      set check-ssl-version {enable | disable}
      set dane-support {mandatory | none | opportunistic}
      set encryption-strength <bits_int>
      set min-ssl-version {ssl3 | tls1_0 | tls1_1 | tls1_2 | tls1_3}
      set mtasts-status {enable | monitor | none}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the TLS profile.	
level {none | preferred | secure}	Enter the security level of the TLS connection. • `none`: Disables TLS. Requests for a TLS connection will be ignored. • `preferred`: Allow a simple TLS connection, but do not require it. Data is not encrypted, nor is the identity of the server validated with a certificate. • `secure`: Requires a certificate-authenticated TLS connection. CA certificates must be installed on the FortiMail unit before they can be used for secure TLS connections. For information on installing CA certificates, see the FortiMail Administration Guide.	none
action {fail | tempfail}	Select the action the FortiMail unit takes when a TLS connection cannot be established. This option does not apply if `level` is `preferred`.	tempfail
ca-name <ca_name>	Enter the name of the CA issuer. This option is only available when `level` is set to `secure`.	
cert-subject <subject_str>	Enter the certification subject. This option is only available when `level` is set to `secure`.	

Variable	Description	Default
check-ca-name {enable | disable}	Enable to check the CA issuer name. This option is only available when `level` is set to `secure`.	disable
check-ca-type {match | substring | wildcard}	Select a CA issuer check type. This option is only available when `level` is `secure`.	match
check-cert-subject {enable | disable}	Enable to check the certificate subject name. This option is only available when `level` is `secure`.	disable
check-cert-type {match | substring | wildcard}	Select a certificate check type. This option is only available when `level` is `secure`.	match
check-encryption-strength {enable | disable}	Enable to check encryption key length.	disable
check-ssl-version {enable | disable}	Enable to check the SSL/TLS version. Also configure min-ssl-version {ssl3 | tls1_0 | tls1_1 | tls1_2 | tls1_3}.	disable
dane-support {mandatory | none | opportunistic}	Assign a DNS-based Authentication of Named Entities (DANE) support level. **Note:** `mandatory` is only applicable when `level` is `secure`. For more information, see RFC 7929.	none
encryption-strength <bits_int>	Enter the encryption key length.	256
min-ssl-version {ssl3 | tls1_0 | tls1_1 | tls1_2 | tls1_3}	Enter the minimum required SSL/TLS version. This option is only available when `check-ssl-version` is `enable`.	tls1_1
mtasts-status {enable | monitor | none}	Enable MTA Strict Transport Security (MTA-STS) domain checking. This option is only available when `level` is either `preferred` or `secure`. **Note:** The MTA-STS status may only be set when `smtp-mtasts-status` is enabled under system mailserver.	none

Related topics

cloud-api profile antivirus

system mailserver

profile url-filter

Use this command to configure URL filter profiles. URL filter profiles select which rating categories you want to scan, rewrite, or block in email message bodies.

You can configure how FortiMail detects URLs. See url-checking {aggressive | extreme | strict}.

Syntax

```
config profile url-filter
   edit <profile_name>
      [set comment "<comment_str>"]
      set category <category_name>
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile.	
category <category_name>	Select which predefined FortiGuard and/or custom URL categories to use with the profile. To view all available categories, enter: `set category ?`	child-abuse drug-abuse adult-materials nudity-risque pornography spam-urls phishing malicious-web
comment "<comment_str>"	Enter a description or comment.	

Related topics

antispam settings
profile antispam
system fortiguard url-protection
system fortisandbox
system webfilter customized-category
system webfilter local-rating

profile weighted-analysis

Use this command to configure weighted analysis profiles. To avoid false positives and false negatives, you can adjust ("weight") the scores of each type of suspicious behavior, and the total score threshold that an email

must reach to be categorized as spam.

To use a weighted analysis profile, select it in an antispam profile.

Syntax

```
config profile weighted-analysis
   edit <profile_name>
      set comment <comment_str>
      config rule
         edit <order_index>
            set name <rule_name>
            set status {enable | disable}
            set action <profile_name>
            set threshold <score_float>
            set cousin-domain-score <score_float>
            set dictionary-profile <profile_name>
            set dictionary-threshold <limit_int>
            set action-keyword-score <score_float>
            set intelligent-analysis-score <score_float>
            set malformed-email-score <score_float>
            set relationship-strong-score <threshold_int>
            set relationship-weak-score <threshold_int>
            set sender-alignment-score <score_float>
            set suspicious-character-score <score_float>
            set url-profile <profile_name>
            set url-profile-score <score_float>
         next
      end
end
```

Variable	Description	Default
<profile_name>	Enter the name of the weighted-analysis profile.	
comment <comment_str>	Enter a descriptive comment.	
<order_index>	Enter the numerical order of the rule in the profile.	
name <rule_name>	Enter a name for the rule.	
status {enable | disable}	Enable or disable the rule.	enable
action <profile_name>	Enter the name of an action profile.	
threshold <score_float>	Enter the minimum total score that triggers the `action`. The total score is determined by adding all weighted scores in the rule (`cousin-domain-score`, etc.).	50.000000

Variable	Description	Default
cousin-domain-score <score_float>	Enter a weight-adjusted score for domain name impersonation.	10.000000
dictionary-profile <profile_name>	Enter the name of a dictionary profile that contains words or phrases that typically only spam has. Keywords are often a "call to action" that motivates the user to reply or click a hyperlink. For example, "Click here", "transfer", "money", "dollars", "bank account", "conference attendee", etc.	
dictionary-threshold <limit_int>	Enter the threshold for dictionary profile matches. When the dictionary profile scans an email, it counts the number of matching words or phrases, and adjusts this total according to pattern-weight <weight_int> and pattern-max-weight <weight_int>. If the result equals or exceeds this threshold, then FortiMail applies the weighted score defined in action-keyword-score <score_float>.	1
action-keyword-score <score_float>	Enter a weight-adjusted score to apply if an email equals or exceeds the limit in dictionary-threshold <limit_int>.	10.000000
intelligent-analysis-score <score_float>	Enter a weight-adjusted score for intelligent analysis detections. Multiple factors contribute to intelligent spam analysis in order to reduce false positives, including: • SPF • DKIM • DMARC • matching of sender addresses in the message headers (`From:` and `Reply-To:`) • newly registered domain names that do not have a FortiGuard Antispam rating yet • header analysis • malformed email detection	50.000000
malformed-email-score <score_float>	Enter a weight-adjusted score for malformed emails. Malformed emails are those emails that contain malformed data in the email structure, header, or body. For more information, see RFC 7103.	10.000000
relationship-strong-score <threshold_int>	Enter the score for strong or weak relation result obtained from querying FortiGuard Sender and Recipient Relationship (SRR). FortiGuard Social Database contains the social mapping of the email communication flow. For example, if user1@1.example.com and user2@2.example.com have regular communication, then their SRR is strong; if they have no history of communication before, then their SRR is weak.	-30.000000

Variable	Description	Default
relationship-weak-score <threshold_int>	Enter the score for weak relation result obtained from querying FortiGuard Sender and Recipient Relationship (SRR).	20.000000
sender-alignment-score <score_float>	Enter a weight-adjusted score for sender domain mismatches. Sender alignment compares the message header (`From:` and `Reply-to:`) with the SMTP envelope (`MAIL FROM:`) to look for a mismatch, which is typical of spam.	10.000000
suspicious-character-score <score_float>	Enter a weight-adjusted score for suspicious characters. Detects internationalized domain name (IDN) homograph attacks. If domain names in URLs, sender email addresses, or recipient email addresses have Unicode characters that are from different languages yet look similar (for example, `A` looks similar in Cyrillic, Greek, and Latin alphabets), then an attacker could trick the user into using a fraudulent website or email. FortiMail detects these as suspicious.	10.000000
url-profile <profile_name>	Enter the name of a URL profile detect spam or phishing hyperlinks in email.	unrated
url-profile-score <score_float>	Enter a weight-adjusted score for email with spam or phishing URLs.	10.000000

Related topics

profile antispam

profile cousin-domain

profile dictionary

profile url-filter

report domain-mail-stats

Use this command to configure domain-level mail statistics report.

Syntax

```
config report domain-mail-stats
   set status {enable | disable} on page 268
   set report-by-email {enable | disable} on page 268
   set domains {all | <protected-domain_str>} on page 268
```

```
    set schedule-frequency {daily | monthly | weekly} on page 268
    set schedule-hour <hour_int> on page 268
end
```

Variable	Description	Default
status {enable | disable}	Enable to generate domain mail statistics reports.	disable
report-by-email {enable | disable}	Enable to send report emails for selected domains	disable
domains {all | <protected-domain_str>}	Enter either `all` to include all protected domains in the report, or enter a list of one or more protected domains. Separate each protected domain with a comma (,).	all
schedule-frequency {daily | monthly | weekly}	Frequency of the scheduled report.	monthly
schedule-hour <hour_int>	Hour of the day to generate the report, between 0 - 23.	23

report mail

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

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

Syntax

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

```
        set schedule-weekdays <days_str>
        set sender-domains
    end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile.	
dest-ip-mask <ip/netmask_str>	Enter the IP address to which reports on logged email messages are destined.	0.0.0.0/32
dest-ip-type {ip-group | ip-mask}	Enter the type of the IP address for sending reports on logged email messages.	ip-mask
direction {both | incoming | outgoing}	Enter one of the following: • `both`: Report on both incoming and outgoing email. • `incoming`: Report only on email whose recipient is a member of a protected domain. • `outgoing`: Report only on email whose recipient is **not** a member of a protected domain.	both
domains {all | <protected-domain_str>}	Enter either `ALL` to include all protected domains in the report, or enter a list of one or more protected domains. Separate each protected domain with a comma (,).	all
file-format {html | pdf}	Enter the file format of the generated report.	pdf
period-absolute-from <start_str>	Enter the beginning of the time range in the format yyyy-mm-dd-hh, where yyyy is the year, mm is the month, dd is the day, and hh is the hour in 24-hour clock format. For example, entering `2008-10-24-09` includes log messages as early as 9 AM on October 24, 2008.	
period-absolute-to <end_str>	Enter the end of the time range in the format yyyy-mm-dd-hh, where yyyy is the year, mm is the month, dd is the day, and hh is the hour in 24-hour clock format. For example, entering `2009-10-24-17` includes log messages as late as 5 PM on October 24, 2009.	
period-relative {last-2-weeks | last-7-days | last-14-days | last-30-days | last-N-days | last-N-hours | last-N-weeks | last-month | last-quarter | last-week | not-used | this-month | this-quarter | this-week | this-year | today | yesterday}	Enter the time span of log messages from which to generate the report. If you entered `last-N-days`, `last-N-hours`, or `last-N-weeks` also configure `period-relative-value <n_int>`.	

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

Variable	Description	Default
schedule-weekdays <days_str>	Enter the days to generate the reports. Separate each day with a comma (,). For example, to generate a report on Friday and Wednesday, you would enter `wednesday,friday`.	
sender-domains	Enter the selected sender domain names (empty means ALL)	

Related topics

log alertemail setting

report mailbox

Note that this command is only available when `mailbox-service` is enabled under system global.

Use this command to configure mailbox report schedules.

The mailbox service feature is license based. This command is only available with a valid purchased advanced management license from FortiGuard.

Syntax

```
config report mailbox
   edit <report_name>
      set domains <domain_str>
      set mailbox-list {enable | disable}
      set period {last_month | this_month | today |  yesterday}
      set recipients <email_addr_str>
      set schedule-frequency {daily | monthly | none | weekly}
      set schedule-hour <hour_int>
      set schedule-weekdays {friday | monday |  saturday | sunday | thursday | tuesday |
          wednesday}
      set schedule-dates {1 | 2 | ... | 30 | 31}
 end
```

Variable	Description	Default
<report_name>	Enter the name of the mailbox report schedule.	
domains <domain_str>	List of domains to be reported.	

Variable	Description	Default
mailbox-list {enable | disable}	Enable to include mailbox lists in reports.	disable
period {last_month | this_month | today | yesterday}	Period of report coverage.	today
recipients <email_addr_str>	List of email recipients of the report.	
schedule-frequency {daily | monthly | none | weekly}	Frequency of the scheduled report.	none
schedule-hour <hour_int>	Hour of the day to generate the report, between 0 - 23.	12
schedule-weekdays {friday | monday | saturday | sunday | thursday | tuesday | wednesday}	**Note**: This option is only available when `schedule-frequency` is set to `weekly`. Days of the week to generate the report.	
schedule-dates {1 | 2 | ... | 30 | 31}	**Note**: This option is only available when `schedule-frequency` is set to `monthly`. Dates of the month to generate the report.	

sensitive data

Use this command to configure sensitive data.

Syntax

```
config sensitive-data fingerprint
      edit <fingerprint data name>
         config document
            edit <document id>
               set filename
               set signature
config sensitive-data fingerprint-source
      edit <DLP server name>
         set file-path
         set file-pattern
         set keep-modified
         set password
         set period
         set remove-deleted
         set scan-subdirectories
         set server
         set server-type
         set username
      edit linux
         set file-path
         set file-pattern
         set keep-modified
```

```
            set password
            set period
            set remove-deleted
            set scan-subdirectories
            set server
            set server-type
            set username
end
```

Variable	Description	Default
<fingerprint data name>	Enter the name of the fingerprint data you want to configure.	
document	Enter to examine a list of created document IDs.	
<document id>	Enter the name of the document you want to modify.	
filename	Enter the filename of the fingerprint document.	
signature	Enter the signature of the file.	
fingerprint-source	Enter to configure the fingerprint source.	
<DLP server name>	Enter the name of the DLP server.	
linux	Enter the Linux identifier.	
file-path	Enter the file path on the server.	
file-pattern	Enter the file patterns to fingerprint.	
keep-modified	Keep previous fingerprints for modified files (enable or disable).	
password	Enter the login password.	
period	Select periodic server checking.	
remove-deleted	Remove fingerprints for deleted files (enable or disable).	
scan-subdirectories	Fingerprint files in subdirectories (enable or disable).	
server	Enter the IP address of the server.	
server-type	Enter the DLP server type.	
username	Enter the login username.	

system accprofile

Use this command to configure access profiles that, in conjunction with the domain or system-wide access level, govern whether or not an administrator account has permissions to view, change, or use features in each functional area. For details, see the FortiMail Administration Guide.

Syntax

```
config system accprofile
   edit <profile_name>
```

```
        set comment <description_str>
        config menuitem
           edit {archive_grp | cluster_grp | content_grp | dashboard_grp | domain_grp | encryption_
                 grp | fortiview_grp | log_grp | monitor_grp | ms365_grp | others_grp | policy_grp |
                 profile_grp | security_grp | system_grp}
              set permission {custom | none | read | read-write}
              set content-detail {enable | disable}
           next
        end
        set granular-group {all}
        set privilege-level {high | low | medium}
        set system-diagnostics {enable | disable}
        set system-quarantine-folder {none | read | read-write}
end
```

Variable	Description	Default
<profile_name>	Enter the name of the access profile.	
comment <description_str>	Enter a descriptive comment.	
{archive_grp | cluster_grp | content_grp | dashboard_grp | domain_grp | encryption_grp | fortiview_grp | log_grp | monitor_grp | ms365_grp | others_grp | policy_grp | profile_grp | security_grp | system_grp}	Enter the name of the functional area that you want to grant permissions for. For example, SAML SSO settings are in multiple areas of the CLI and GUI. Therefore administrators that configure SSO require `read-write` or `read-update` permissions for all of these: • `domain_grp` • `profile_grp` • `system_grp`	
permission {custom | none | read | read-write}	Grant a permission for features in the functional area. `read-update` is like `read-write`, except new tables (profiles etc.) cannot be created and existing ones cannot be deleted.	none
content-detail {enable | disable}	Enable or disable administrators with *Read* privileges or better to be able to view email contents. **Note:** This setting is only available for `archive_grp`.	enable
granular-group {all}	Enter the permission for granular control.	all
privilege-level {high | low | medium}	Set the access profile's privilege level. Administrators with a `low` privilege level cannot use `diagnose` or `config system` CLI commands.	medium
system-diagnostics {enable | disable}	Enable or disable permission to run system diagnostic commands.	enable
system-quarantine-folder {none | read | read-write}	For system quarantine, enter the permissions that will be granted to administrator accounts associated with this access profile.	none

Related topics

system admin

system admin

Use this command to configure FortiMail administrator accounts.

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

Syntax

```
config system admin
   edit <name_str>
      set status {enable | disable}
      set access {cli | gui | rest}
      set access-profile <profile_name>
      set auth-strategy {cloud | ldap | local | pki | radius | sso}
      set language <language_name>
      set level {domain | domain-group | system}
      set ldap-profile <profile_name>
      set password <password_str>
      set pkiuser <pkiuser_name>
      set radius-profile <profile_name>
      set sshkey <key_str>
      set sso-profile <profile_name>
      set theme {Blue |Green | Light-Blue | Neutrino | Red}
      set trusted-hosts <host_ipv4mask>
      set webmode {advanced | cloud-api | simple}
end
```

Variable	Description	Default
<name_str>	Enter the name of the administrator account.	
status {enable | disable}	Enable to activate the administrator account.	disable
access {cli | gui | rest}	Select the access method allowed for the administrator. Access methods require that you also enabled the associated protocols on the network interface where the administrator connects.	cli gui rest
access-profile <profile_name>	Enter the name of an access profile that determines which functional areas the administrator account is allowed to view or affect.	

Variable	Description	Default
auth-strategy {cloud | ldap | local | pki | radius | sso}	Select the type of authentication profile that the administrator account will use to log in. (The `cloud` option is FortiCloud.) If you did not select `local`, then you must also select the name of the profile to use in a separate setting such as ldap-profile <profile_name>.  The GUI login page may not include all types, depending on what you select for admin-sso-login-option {normal | sso-only} on page 280.	local
language <language_name>	Enter this administrator account's preference for the display language of the GUI. Available languages vary by whether or not you have installed additional language resource files. To view a list of languages, enter a question mark (`?`).	english
level {domain | domain-group | system}	Select the administrator's access level.	system
ldap-profile <profile_name>	If `auth-strategy` is `ldap`, enter the LDAP profile that you want to use.	
password <password_str>	If `auth-strategy` is `local` or `radius`, enter the password for the administrator account.  Do not enter a FortiMail administrator password less than 8 characters long. For better security, enter a longer password with a complex combination of characters and numbers, and change the password regularly. Failure to provide a strong password could compromise the security of your FortiMail unit.	
pkiuser <pkiuser_name>	If `auth-strategy` is `pki`, enter the name of a PKI user.	
radius-profile <profile_name>	If `auth-strategy` is `radius`, enter the name of a RADIUS authentication profile that you want to use.	
sshkey <key_str>	Enter the SSH public key string surrounded in single straight quotes (`'`). When connecting from an SSH client that presents this key, the administrator will not need to provide their account name and password in order to log in to the CLI.	
sso-profile <profile_name>	If `auth-strategy` is `sso`, enter the SSO profile that you want to use.	

Variable	Description	Default
theme {Blue |Green | Light-Blue | Neutrino | Red}	Enter this administrator account's preference for the display theme when logging in.	Green
trusted-hosts <host_ipv4mask>	Enter one to three IP addresses and netmasks from which the administrator can log in to the FortiMail unit. Separate each IP address and netmask pair with a comma (,). To allow the administrator to authenticate from any IP address, enter `0.0.0.0/0.0.0.0`.	0.0.0.0/0.0.0.0
webmode {advanced | cloud-api | simple}	Enter which display mode will initially appear when the administrator logs in to the GUI. The administrator can switch the display mode during their session; this setting only affects the initial state of the display.	simple

Related topics

profile authentication
profile ldap
profile sso
sensitive data
system accprofile
system appearance
system interface
system web-service
user pki

system advanced-management

Use this command to control advanced management features that are designed for deployments such as managed security service providers (MSSP).

Advanced management options require a valid feature license, purchased from Fortinet.

Some subcommands are only available when MTA advanced control is enabled. See mta-adv-ctrl-status {enable | disable} on page 313

Syntax

```
config system advanced-management
   set dmarc-report-analysis-status {enable | disable}
   set domain-admin-log-status {enable | disable}
   set domain-group-status {enable | disable}
   set domain-mail-stats-status {enable | disable}
   set ha-central-monitor-status {enable | disable}
   set intra-domain-protection-status {enable | disable}
   set mailbox-accounting-status {enable | disable}
   set user-management {enable | disable}
end
```

Variable	Description	Default
dmarc-report-analysis-status {enable | disable}	Enable or disable collection of statistics about DMARC reports, such as how many email were sent to a recipient domain, and how many failed DMARC verification. To view the statistics, on the GUI, go to *Monitor* > *DMARC Analysis* > *Analysis Summary* or *Monitor* > *DMARC Analysis* > *Analysis Detail*. Alternatively, you can enable or disable this for each protected domain. See dmarc-report-analysis-status {enable | disable | use-system-setting} on page 91. To enable DMARC reports, see antispam dmarc-report-generation on page 45.	disable
domain-admin-log-status {enable | disable}	Enable or disable domain-level administrator log access.	enable
domain-group-status {enable | disable}	Enable or disable domain group support.	enable
domain-mail-stats-status {enable | disable}	Enable or disable domain-level mail statistics.	disable
ha-central-monitor-status {enable | disable}	Enable or disable HA central monitoring.	disable
intra-domain-protection-status {enable | disable}	Enable or disable applying both inbound and outbound policies when an email is sent between protected domains.	disable

Variable	Description	Default
	When this setting is disabled, if an email is sent between two protected domains, then FortiMail only applies the matching inbound policy. This means that, for example, an inbound policy with antispam would apply, but not an outbound policy with DLP. This behavior may be correct if all protected domains belong to the same company. However for an MSSP with multiple tenants, both policies should apply. In that case, enabled this setting so that FortiMail applies **both** inbound and outbound policies.	
mailbox-accounting-status {enable | disable}	Enable or disable the mailbox accounting service.	disable
user-management {enable | disable}	Enable or disable user management.	disable

Related topics

antispam dmarc-report-generation

report mailbox

system domain-group

system global

system ha

system appearance

Use this command to customize the appearance of the GUI for administrators and FortiMail webmail users.

Syntax

```
config system appearance
   [set comment "<comment_str>"]
   set admin-sso-login-option {normal | sso-only}
   set customized-login-status {enable | disable}
   set fallback-charset {Big5 | ... | Windows-1256}
   set login-page-language <language_name>
   set login-page-theme {Blue | Dark | Green | Light-Blue | Neutrino | Red}
   set product <product-name_str>
   set webmail-help-status {enable | disable)
```

```
    [set webmail-help-url "<webmail-help_url>"]
    set webmail-lang <language_name>
    set webmail-login "<login-page-title_str>"
    set webmail-login-hint "<hint_str>"
    set webmail-sort-option {order-received | time-received}
    set webmail-sso-login-option {normal | sso-only}
    set webmail-theme {Blue | Dark | Green | Light-Blue | Neutrino | Red}
    set webmail-theme-status {enable | disable}
end
```

Variable	Description	Default
admin-sso-login-option {normal | sso-only}	Select which authentication methods to show on the GUI login page for administrators: • `normal`: Show both the username and password fields, and a single sign-on (SSO) link. • `sso-only`: Show only the SSO link. **Caution:** If you select this option, then the account named `admin` will not be able to log into the GUI; they must use SSH or local console access instead. Therefore this option can only be changed by administrators with the `super_admin_prof` permissions profile. To authenticate each administrator, FortiMail uses the remote servers (if any) selected in auth-strategy {cloud | ldap | local | pki | radius | sso} on page 276.	normal
comment "<comment_str>"	Enter a description or comment.	
customized-login-status {enable | disable}	Enable to edit a graphic that will appear at the top of all webmail pages. The image's dimensions must be 314 pixels wide by 36 pixels tall.	disable
fallback-charset {Big5 | ... | Windows-1256}	Enter the fallback character set for email that are not RFC 2047 compliant . To display the full list of options, enter: `set fallback-charset ?`	
login-page-language <language_name>	Enter the default language for the display of the login page of the GUI. To view a list of languages, enter a question mark (`?`). **Note:** The setting only affects the login page, not the entire GUI.	english
login-page-theme {Blue | Dark | Green | Light-Blue | Neutrino | Red}	Select the display color theme of the login page.	Green
product <product-name_str>	Enter the text that will precede 'Administrator Login' on the login page.	FortiMail
webmail-help-status {enable | disable)	Enable to display the help button (**?**) in webmail.	enable

Variable	Description	Default
webmail-help-url "<webmail-help_url>"	If you want to provide your own custom help to webmail users, enter its URL. Otherwise the default webmail help is provided by Fortinet.	
webmail-lang <language_name>	Enter the name of a language in English, such as `'French'`, that will be used when an email user initially logs in to FortiMail webmail. The email user may switch the display language in their preferences; this affects only the initial state of the display. Available language names vary by whether or not you have installed additional language resource files.	English
webmail-login "<login-page-title_str>"	Enter a word or phrase that will appears at the top of the webmail login page. Surround the value with quotes if it contains a space or special character.	"Webmail Login"
webmail-login-hint "<hint_str>"	Enter a hint for the user name. This hint will appear when you hover the mouse cursor over the login name field.	"Input your email address"
webmail-sort-option {order-received | time-received}	Select how webmail will sort email: • `order-received`: Sorted by the order in which emails are delivered to the mailbox folder. • `time-received`: Sorted by the time that emails are received by the mail server.	time-received
webmail-sso-login-option {normal | sso-only}	Select which authentication methods to show on the GUI login page for webmail users: • `normal`: Show both the username and password fields, and a single sign-on (SSO) link. • `sso-only`: Show only the SSO link.	normal
webmail-theme {Blue | Dark | Green | Light-Blue | Neutrino | Red}	Select a default color theme for the webmail and quarantine GUI after users log in. Alternatively, you can set this default for each domain (webmail-theme {Blue | Dark | Green | Light-Blue | Neutrino | Red | Use-system-setting}). If webmail-theme-status {enable | disable} is `enable`, then after they log in, each user may choose a different theme.	Blue
webmail-theme-status {enable | disable}	Enable for users to be able to change their webmail GUI theme.	enable

Related topics

domain-setting
system admin
system geoip-override
system saml
system webmail-language

system backup-restore-mail

Use this command to configure the storage media and schedule for backups of email user's mailboxes.

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

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

Syntax

```
config system backup-restore-mail
   set encryption-key <key>
   set folder <path_str>
   set full <full-backups_int>
   set host <fortimail_fqdn>
   set hour-of-day <hours_int>
   set monthly-day-of-month
   set monthly-incremental-days
   set number-of-backups
   set port <port_int>
   set protocol {ext-usb | ext-usb-auto | iscsi_server | nfs | smb-winserver | ssh}
   set status {enable | disable}
end
```

Variable	Description	Default
encryption-key <key>	Enter the encryption key for backup/restore.	
folder <path_str>	Enter the path of the folder on the backup server where the FortiMail unit will store the mailbox backups, such as: `/home/fortimail/mailboxbackups` This field appears only if the backup media is an NFS server or SSH server.	FortiMail-mail-data-backup
full <full-backups_int>	Enter the total number of full backups to keep on the backup media. Valid values are between 1 and 10.	3
host <fortimail_fqdn>	If you want to restore all mailboxes from a backup labeled with the fully qualified domain name (FQDN) of a previous FQDN, or that of another FortiMail unit, enter the FQDN of the backup that you want to restore. For example, to restore the most recent backup made by a FortiMail unit named fortimail.example.com, enter `fortimail.example.com`.	
hour-of-day <hours_int>	Enter the hour of the day, according to a 24-hour clock, on the days of the week at which to make backups. For example, to make backups at 9 PM, enter `21`.	23

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

Related topics

backup-restore

system link-monitor

system certificate ca

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

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

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

Syntax

```
config system certificate ca
   edit <certificate_name>
      set certificate <certificate_str>
end
```

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

Related topics

system certificate crl

system certificate local

system certificate remote

system certificate crl

Use this command to import certificate revocation lists.

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

Syntax

```
config system certificate crl
   edit <certificate_name>
      set crl <certificate_str>
```

```
end
```

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

Related topics

system certificate local
system certificate remote

system certificate local

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

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

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

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

Syntax

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

Variable	Description	Default
<certificate_name>	Enter a name for the certificate to be imported.	

Variable	Description	Default
password	Enter a password for the certificate.	
private-key	Enter a private key for the certificate. **Note**: A random password is used to encrypt the private key, to prevent the private key from becoming visible when using the `show` command.	
certificate <certificate_str>	Enter or paste the certificate in PEM format to import it.	
csr <csr_str>	Enter or paste the certificate signing request in PEM format to import it.	
comments <comment_str>	Enter any comments for this certificate.	

Related topics

system certificate crl

system certificate remote

system certificate remote

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

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

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

Syntax

```
config system certificate remote
   edit <certificate_name>
      set certificate <certificate_str>
end
```

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

Related topics

system certificate crl
system certificate local

system config-control

Use this command to configure control and table templates.

Syntax

```
config system config-control
   set base-config-name <string>
   set base-config-status {enable | disable}
   set domain-admin-restriction {enable | disable}
end
```

Variable	Description	Default
base-config-name <string>	Enter the name of the base table entry that the new table entry will take values from.	
base-config-status {enable | disable}	Enable to allow table entry creation, such as antispam profiles, to take values from `base-config-name`.	enable
domain-admin-restriction {enable | disable}	Enable to restrict domain-level administrators from making changes to certain settings.	disable

system csf

Use this command to configure the FortiMail unit as a FortiGate Security Fabric member.

Syntax

```
config system csf
   set configuration-sync {local | sync}
   set group-name <name_str>
   set group-password <password_str>
   set management-ip <address_ipv4>
   set management-port <port_int>
   set status {enable | disable}
   set upstream-ip <address_ipv4>
```

```
    set upstream-port <port_int>
end
```

Variable	Description	Default
configuration-sync {local | sync}	Select the configuration synchronization mode.	local
group-name <name_str>	Enter the Security Fabric group name.	
group-password <password_str>	Enter the password for the Security Fabric group.	
management-ip <address_ipv4>	Enter the management IP address.	
management-port <port_int>	Enter the port number where the unit listens for Security Fabric communications. Valid range is 1-65535.	443
status {enable | disable}	Enable or disable Security Fabric configuration.	enable
upstream-ip <address_ipv4>	Enter the IP address of upstream.	172.20.141.151
upstream-port <port_int>	Enter the upstream port number.	8013

Related topics

system certificate crl

system certificate local

system ddns

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

Syntax

```
config system ddns
   edit <ddns-service_str>
      config domain
         edit domain <domain_str>\
            set ipmode {auto | bind | static}
            set interface <interface_str>
            set ip <host_ipv4>
            set status {enable | disable}
```

```
            set type {custom | dynamic | static}
        set password <password_str>
        set timeout <time_int>
        set username <username_str>
    end
```

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

Related topics

system dns

system disclaimer

Use this command to configure system-wide disclaimer messages.

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

Disclaimer messages can be appended for either or both incoming or outgoing email messages. For information on determining the directionality of an email message, see the FortiMail Administration Guide.

Syntax

```
config system disclaimer
   set exclude-status {enable | disable}
   set disclaimer-status {enable | disable}
end
```

Variable	Description	Default
exclude-status {enable | disable}	Enable if you do not want to insert disclaimers to the email messages from certain senders or to certain recipients. Also configure system disclaimer-exclude on page 291.	disable
disclaimer-status {enable | disable}	Enable to insert customized disclaimer messages for incoming and/or outgoing email. Also configure system disclaimer-message on page 291 and disclaimer-per-domain {enable | disable}.	disable

Related topics

policy ip
policy recipient
system disclaimer-exclude
system disclaimer-message
system global

system disclaimer-exclude

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

Syntax

```
config system disclaimer-exclude
   edit <profile_index>
      set recipient-pattern <recipient_pattern>
      set sender-pattern <sender_pattern>
      set source-ip <source_ipv4/mask>
end
```

Variable	Description	Default
<profile_index>	Enter a number for the exclusion.	
recipient-pattern <recipient_pattern>	Enter a recipient pattern. For example, if you add *@example.com, all messages to example.com users will be exempted from disclaimer insertion.	*
sender-pattern <sender_pattern>	Enter a sender pattern. For example, if you add *@example.com, all messages from example.com users will be exempted from disclaimer insertion.	*
source-ip <source_ipv4/mask>	Define the source IP address and netmask to exclude from disclaimers.	0.0.0.0/0

Related topics

system disclaimer

system disclaimer-message

Use this command to configure system-wide disclaimer messages.

If disclaimer-per-domain {enable | disable} is enabled, then you can configure disclaimer messages that are specific to each protected domain. See disclaimer-status {disabled | use-domain-setting | use-system-setting} on page 90.

Syntax

```
config system disclaimer-message
   edit <profile_index>
      set status {enable | disable}
      set sender-domain-type {all | external | internal}
      set recipient-domain-type {all | external | internal}
      set relationship-strength-status {enable | disable}
      set relationship-strength {neutral | strong | weak}
      set customized-message {default | incoming-system-disclaimer | outgoing-system-disclaimer}
end
```

Variable	Description	Default
<profile_index>	Enter a number for the disclaimer message.	
customized-message {default | incoming-system-disclaimer | outgoing-system-disclaimer}	Select which customized message to use. Also configure customized-message on page 80.	default
recipient-domain-type {all | external | internal}	Select which type of recipient domains will have the disclaimer message applied to their email.	internal
relationship-strength {neutral | strong | weak}	Select the relationship strength level to apply the disclaimer message. FortiGuard Social Database contains the social mapping of the email communication flow. For example, if user1@1.example.com and user2@2.example.com have regular communication, then their SRR is strong; if they have no history of communication before, then their SRR is weak.	weak neutral strong
relationship-strength-status {enable | disable}	Enable or disable relationship strength as a factor for deciding whether to apply the disclaimer message.	disable
sender-domain-type {all | external | internal}	Select which type of sender domains will have the disclaimer message applied to their email.	external
status {enable | disable}	Enable or disable the disclaimer message. This applies only to the individual message. To enable or disable the disclaimer message feature, see system disclaimer.	disable

Related topics

system disclaimer

domain

customized-message

system dns

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

You can also configure up to three other DNS servers for protected domains' (and their domain associations) MX record query only. This is useful if the protected domains' MX record or A record are resolved differently on internal DNS servers. This feature is only applicable to gateway mode and transparent mode and when you select MX record as the relay type in domain settings.

Note that if you configure DNS servers for protected domains (such as example.com), FortiMail will also use the same DNS server for all queries that are in the form of anysub.example.com, so that the recursive queries for the returned MX record (mx.example.com) or other records can be directed to the same server.

Syntax

```
config system dns
   set cache {enable | disable}
   set cache-min-ttl <time-in-seconds>
   set primary <ipv4_address>
   set protected-domain-dns-servers <ipv4_address>
   set protected-domain-dns-state {enable | disable}
   set ptr-query-option {enable |  disable| public-ip-only}
   set secondary <dns_ipv4>
   set truncate-handling {disable | tcp-retry}
end
```

Variable	Description	Default
cache {enable | disable}	Enable to cache DNS query results to improve performance. Disable the DNS cache to free memory if you are low on memory.	enable
cache-min-ttl <time-in-seconds>	Use this command to overwrite the TTL of the cached DNS records in case the TTL of the records is very short. However, the newly set TTL value is only effective if it is longer than the original TTL. For example, if you set it to 30 seconds while the original TTLis 10 seconds, then the actual record TTL will become 30 seconds. If you set it to 30 seconds while the original TTL is 60 seconds, then the actual record TTL remains to be 60 seconds.	300
primary <ipv4_address>	Enter the IP address of the primary DNS server.	0.0.0.0
protected-domain-dns-servers <ipv4_address>	Enter the IP address of the DNS servers that you want to use to resolve the protected domain names (including their subdomains) and the MX Record (alternative domain). You can enter up to 3 addresses/DNS servers.	0.0.0.0

Variable	Description	Default
protected-domain-dns-state {enable | disable}	Either enable or disable the protected domain DNS servers.	disable
ptr-query-option {enable | disable| public-ip-only}	Enable to perform reverse DNS lookups on both private network IP addresses and public IP addresses. However, PTR queries may cause delays when the DNS server has no response. In this situation, you may choose to disable the querying. In some cases, the DNS server may not have PTR records for your private network's IP addresses. Failure to contain records for those IP addresses may increase DNS query time. In this situation, you can choose to query on public IP addresses only.	public-ip-only
secondary <dns_ipv4>	Enter the IP address of the secondary DNS serve.	0.0.0.0
truncate-handling {disable | tcp-retry}	Specify how to handle trunctated UDP replies of DNS queries: select either disable (meaning no retries) or tcp-try (meaning retry in TCP mode).	tcp-retry

Related topics

system ddns

system domain-group

The configuration of domain groups for administrators is license based. If you do not purchase the advanced management license, this feature is not available.

Use this command to associate a domain-level administrator to a domain group, allowing administrators to potentially manage multiple domains and all associated log entries.

Syntax

```
config system domain-group
   edit <id>
      set domain <string>
end
```

Variable	Description	Default
<id>	Enter a table ID.	
domain <string>	Enter the domain name(s) that you want to associate to the current administrator.	

Related topics

system encryption ibe

system encryption ibe

Use this command to configure Identity-Based Encryption (IBE) services for encrypted email messages.

Syntax

```
config system encryption ibe
   set account-notification {activation deletion expiration registration-confirmation reset-
       confirmation}
   set auth-mode {password | token | two-factor}
   set custom-user-control-status {enable | disable}
   set expire-alert <days_int>
   set expire-emails <days_int>
   set expire-inactivity <days_int>
   set expire-passwd-reset <hours_int>
   set expire-registration <days_int>
   set read-notification {enable | disable}
   set secure-compose {enable | disable}
   set secure-reply {enable | disable}
   set secure-forward {enable | disable}
   set secure-token-ttl <minutes>
   set service-name <name_str>
   set sms-account-id <account-id_str>
   set sms-auth-key <key_str>
   set sms-from-number <number>
   set sms-provider <sms-provider_name>
   set status {enable | disable}
   set two-factor-auth-max-attempt <attempts_int>
   set two-factor-auth-method {email | sms}
   set unread-days <days_int>
   set unread-notif-rcpt <to_email>
   set unread-notif-sender <from_email>
   set unread-notification {enable | disable}
   set url-about <about_url>
   set url-base <base_url>
   set url-custom-user-control <user-check_url>
   set url-forgot-pwd <forgot-password_url>
```

```
    set url-help <help_url>
end
```

Variable	Description	Default
account-notification {activation deletion expiration registration-confirmation reset-confirmation}	Enter the type(s) of account notifications that you want to send to users. Separate multiple options with a space.	activation expiration
auth-mode {password | token | two-factor}	Select the IBE user authentication mode.	password
custom-user-control-status {enable | disable}	If your corporation has its own user authentication tools, enable this option and enter the URL. Also configure url-custom-user-control <user-check_url> and url-forgot-pwd <forgot-password_url>.	disable
expire-alert <days_int>	Enter the number of days before the user account's expiry date to send an alert email notification to the user. The valid range is 0 to 7, where 0 means the account is expired. Optionally, for multiple alert email intervals, separate each entry with a space. For example, the default value (1 7) will send an alert email seven days and one day before the expiry date.	1 7
expire-emails <days_int>	Enter the number of days that the secured mail will be saved on the FortiMail unit.	180
expire-inactivity <days_int>	Enter the number of days the secured mail recipient can access the FortiMail unit without registration. For example, if you set the value to 30 days and if the mail recipient did not access the FortiMail unit for 30 days after they registers on the unit, the recipient will need to register again if another secured mail is sent to them. If the recipient accessed the FortiMail unit on the 15th days, the 30-day limit will be recalculated from the 15th day onwards.	90
expire-passwd-reset <hours_int>	Enter the password reset expiry time in hours. This is for the recipients who have forgotten their login passwords and request for new ones. The secured mail recipient must reset their password within this time limit to access the FortiMail unit.	24
expire-registration <days_int>	Enter the number of days that the secured mail recipient has to register on the FortiMail unit to view the mail before the registration expires. The starting date is the date when the FortiMail unit sends out the first notification to a mail recipient.	30
read-notification {enable | disable}	Enable to send the read notification the first time the mail is read.	disable

Variable	Description	Default
secure-compose {enable | disable}	Select to allow the secure mail recipient to compose an email. The FortiMail unit will use policies and mail delivery rules to determine if this mail needs to be encrypted. For encrypted email, the domain of the composed mail's recipient must be a protected one, otherwise an error message will appear and the mail will not be delivered.	disable
secure-reply {enable | disable}	Allow the secured mail recipient to reply to the email with encryption.	disable
secure-forward {enable | disable}	Allow the secured mail recipient to forward the email with encryption	disable
secure-token-ttl <minutes>	Enter the secure token timeout value in minutes. Valid range is 1-1440.	30
service-name <name_str>	Enter the name for the IBE service. This is the name the secured mail recipients will see once they access the FortiMail unit to view the mail.	
sms-account-id <account-id_str>	Enter the account or service plan ID provided by your SMS provider.	
sms-auth-key <key_str>	The authentication token, or API key, provided by your SMS provider.	
sms-from-number <number>	Enter the phone number from which to send SMS messages.	
sms-provider <sms-provider_name>	SMS provider for two-factor authentication.	twilio
status {enable | disable}	Enable the IBE service you have configured.	disable
two-factor-auth-max-attempt <attempts_int>	Enter the maximum number of attempts a user is allowed for a two-factor authenticated session.	3
two-factor-auth-method {email | sms}	**Note**: This option is only available when auth-mode {password | token | two-factor} iseither `token` or `two-factor`. Enter the verification method for two-factor authentication: email or SMS.	email
unread-days <days_int>	**Note**: This option is only available when unread-notification {enable | disable} is `enable`. Enter the unread notification days.	14
unread-notif-rcpt <to_email>	**Note**: This option is only available when unread-notification {enable | disable} is `enable`. Enable to send the unread notification to the recipient.	disable
unread-notif-sender <from_email>	**Note**: This option is only available when unread-notification {enable | disable} is `enable`. Enable to send the unread notification to the sender.	disable

Variable	Description	Default
unread-notification {enable | disable}	Enable to send the unread notification if the message remains unread for 14 days by default.	disable
url-about <about_url>	You can create a file about the FortiMail IBE encryption and enter the URL for the file. The mail recipient can click the "About" link from the secure mail notification to view the file. If you leave this option empty, a link for a default file about the FortiMail IBE encryption will be added to the secure mail notification.	
url-base <base_url>	Enter the FortiMail unit URL (for example, https://mail.example.com) where a mail recipient can register or authenticate to access the secured mail.	
url-custom-user-control <user-check_url>	Enter the URL where you can check for user existence. This command is available only if custom-user-control-status {enable | disable} is `enable`.	
url-forgot-pwd <forgot-password_url>	Enter the URL where users get authenticated. This command is available only if custom-user-control-status {enable | disable} is `enable`	
url-help <help_url>	You can create a help file on how to access the FortiMail secure email and enter the URL for the file. The mail recipient can click the "Help" link from the secure mail notification to view the file. If you leave this option empty, a default help file link will be added to the secure mail notification.	

Related topics

system encryption ibe-auth

system encryption ibe-auth

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

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

In both cases, the FortiMail unit will record the domain names of the recipients who register or authenticate with it on *User > IBE User > IBE Domain*.

Use this command to bind domains with LDAP authentication profiles with which the FortiMail unit can query the LDAP servers for authentication, email address mappings, and more. For more information about LDAP profiles, see profile ldap on page 221.

Syntax

```
config system encryption ibe-auth
   edit <id>
      set domain-pattern <string>
      set ldap-profile <profile_name>
      set status {enable | disable}
end
```

Variable	Description	Default
<id>	Enter a table ID.	
domain-pattern <string>	Enter a domain name that you want to bind to an LDAP authentication profile. If you want all IBE users to authenticate through an LDAP profile and do not want other non-LDAP-authenticated users to get registered on FortiMail, you can use wildcard * for the domain name and then bind it to an LDAP profile.	
ldap-profile <profile_name>	Enter a profile name from the available LDAP profile list, which you want to use to authenticate the domain users.	
status {enable | disable}	Enable or disable the rule.	disable

Related topics

system encryption ibe

system fortiguard antivirus

Use this command to configure how the FortiMail unit will retrieve the most recent updates to FortiGuard Antivirus engines, antivirus definitions, and antispam definitions (the heuristic antispam rules only). FortiMail can get antivirus updates either directly from a Fortinet Distribution Network (FDN) server or via a web proxy.

Syntax

```
config system fortiguard antivirus
   set override-server-address <virtual-ip_ipv4>
   set override-server-status {enable | disable}
   set scheduled-update-day <day_int>
   set scheduled-update-frequency {daily | every | weekly}
   set scheduled-update-status {enable | disable}
```

```
    set scheduled-update-time <time_str>
    set tunneling-address <ipv4-or-fqdn>
    set tunneling-password <password_str>
    set tunneling-port <port_int>
    set tunneling-status {enable | disable}
    set tunneling-username <username_str>
    set virus-db {default | extended | extreme}
    set virus-outbreak {disable | enable | enable-with-defer}
    set virus-outbreak-protection-period <minutes_int>
end
```

Variable	Description	Default
override-server-address <virtual-ip_ipv4>	If `override-server-status` is `enable`, enter the IP address of the public or private FortiGuard Distribution Server (FDS) that overrides the default FDS to which the FortiMail unit connects for updates.	
override-server-status {enable | disable}	Enable to override the default FDS to which the FortiMail unit connects for updates.	disable
scheduled-update-day <day_int>	Enter the day of the week at which the FortiMail unit will request updates where the range is from 0-6 and 0 means Sunday and 6 means Saturday.	
scheduled-update-frequency {daily | every | weekly}	Enter the frequency at which the FortiMail unit will request updates. Also configure scheduled-update-day <day_int> and scheduled-update-time <time_str>.	weekly
scheduled-update-status {enable | disable}	Enable to perform updates according to a schedule.	enable
scheduled-update-time <time_str>	Enter the time of the day at which the FortiMail unit will request updates, in the format `hh:mm`, where `hh` is the number of hours and `mm` is the number of minutes after the hour in 15 minute intervals.	01:00
tunneling-address <ipv4-or-fqdn>	If `tunneling-status` is `enable`, enter the IP address or FQDN of the web proxy.	
tunneling-password <password_str>	If `tunneling-status` is `enable`, enter the password of the account on the web proxy.	
tunneling-port <port_int>	If `tunneling-status` is `enable`, enter the TCP port number on which the web proxy listens.	

Variable	Description	Default
tunneling-status {enable | disable}	Enable to tunnel antivirus update requests and FortiGuard antispam queries through a web proxy.	disable
tunneling-username <username_str>	If `tunneling-status` is `enable`, enter the user name of the FortiMail unit's account on the web proxy.	
virus-db {default | extended | extreme}	Depending on your models, FortiMail supports three types of antivirus databases: • `default`: The default FortiMail virus database contains most commonly seen viruses and should be sufficient enough for regular antivirus protection. For the current release, FortiMail VM00 model supports the default virus database only. • `extended`: Some high-end FortiMail models support the usage of an extended virus database, which contains viruses that are not active any more. FortiMail VM01/VM02/200F/400F models support both the default and extended virus databases. • `extreme`: Some high-end models also support the usage of an extreme virus database, which contains more virus signatures than the default and extended databases. For the current release, FortiMail VM04/900F and above models support all three types of virus databases.	default
virus-outbreak {disable | enable | enable-with-defer}	When a virus outbreak occurs, it takes some time for updates to the FortiGuard Antivirus database. Therefore you can choose to defer the delivery of a suspicious email messages, giving time for the update to occur, and then scan the email again. • `disable`: Do not query FortiGuard antivirus service. • `enable`: Query FortiGuard antivirus service. • `enable-with-defer`: If the first query returns no results, defer the email for the specified time and then query again.	enable-with-defer
virus-outbreak-protection-period <minutes_int>	If you set `virus-outbreak` to `enable-with-defer`, specify how many minutes to wait and then perform the second query.	20

Related topics

system fortiguard antispam

update

system fortiguard antispam

Use this command to configure how the FortiMail unit will connect to the FortiGuard servers to query for antispam signatures.

Syntax

```
config system fortiguard antispam
   set status {enable | disable}
   set cache-status {enable | disable}
   set cache ttl <ttl_int>
   set cache-mpercent <percentage_int>
   set query-timeout <timeout_int>
   set threshold-ip-connect {1 | 2 | 3}
   set server-override-status {enable | disable}
   set server-override-ip {<host_fqdn> | <host_ipv4>}
   set port {443 | 53 | 8888}
   set protocol {udp | https}
   set url-redirect-lookup {enable | disable}
   set server-location {any | usa}
   set outbreak-protection-level {disable | high | low | medium}
   set outbreak-protection-period <minutes_int>
   set submission-status {enable | disable}
   set submission-per-domain {enable | disable}
   set submission-retention <days_int>
   set submission-spam-addr <spam-sample_email>
   set submission-ham-addr <not-spam-sample_email>
end
```

Variable	Description	Default
cache-mpercent <percentage_int>	Enter the percentage of memory the antispam cache is allowed to use in percentage. The range is 1-15%.	2
cache-status {enable | disable}	Enable cache and specify the cache time to live (TTL) to improve performance. Also configure cache ttl <ttl_int> and cache-mpercent <percentage_int>.	enable
cache ttl <ttl_int>	Enter the TTL in seconds for cache entries. If the entry is not refreshed before this time, then it expires and is removed from cache.	300
outbreak-protection-level {disable | high | low | medium}	Select the threshold level for spam outbreak protection. Higher levels mean stricter filtering.	medium

Variable	Description	Default
	This feature temporarily holds email for a certain period of time (see `outbreak-protection-period`) if the enabled FortiGuard Antispam check (block-IP and/or URL filter) returns no result. After the specified time interval, FortiMail will query the FortiGuard server for the second time. This provides an opportunity for the FortiGuard antispam service to update its database in cases a spam outbreak occurs. Conversely, in order to reduce the types of email to be deferred for outbreak, set this command to `low`.	
outbreak-protection-period <minutes_int>	Specify how long (in minutes) FortiMail will hold email before it query the FortiGuard server for the second time.	30
port {443 | 53 | 8888}	Enter the port number used to communicate with the FortiGuard Antispam query servers.	53
protocol {udp | https}	Enter the protocol used to communicate with the FortiGuard servers.	https
query-timeout <timeout_int>	Enter the timeout value for the FortiMail unit to query the FortiGuard Antispam query server.	7
server-location {any | usa}	Select which geographic regions of FortiGuard servers to use if required by regulatory compliance or for network performance.	any
server-override-ip {<host_fqdn> | <host_ipv4>}	If server-override-status {enable | disable} is `enable`, enter the IP address of the public or private FortiGuard Antispam query server that overrides the default query server to which the FortiMail unit connects.	
server-override-status {enable | disable}	Enable to override the default FortiGuard Antispam query server to which the FortiMail unit connects to and checks for antispam signatures.	disable
submission-handling-type {admin-review | direct-to-fortiguard}	Select whether you want an administrator to manually review spam sample submissions, or you want them to be sent directly to FortiGuard.	admin-review
submission-per-domain {enable | disable}	If you have multiple protected domains, enable this option to allow domain administrators to view spam sample submissions for their own domain.	disable
submission-ham-addr <not-spam-sample_email>	Enter the email address that will receive samples of normal email (not spam). **Note:** Sample submission email addresses must: • Not be the same. • Be reserved only for samples of spam and non-spam; they should not receive any other email.	

Variable	Description	Default
submission-retention <days_int>	Enter a number of days between 0-60, after which the sample spam submission will be deleted.	14
submission-spam-addr <spam-sample_email>	Enter the email address that will receive samples of spam email. **Note:** Sample submission email addresses must: • Not be the same. • Be reserved only for samples of spam and non-spam; they should not receive any other email.	
submission-status {enable | disable}	Enable to submit samples of spam and non-spam that were not detected correctly to FortiGuard or your FortiMail administrators. This information can be used to improve the catch rate. Users can submit samples of spam and non-spam via the *Report Spam* plugin for Microsoft Outlook. The plugin is available for download at https://support.fortinet.com/. To review the submitted samples, go to *Monitor* > *Quarantine* > *Sample Submission*.	disable
status {enable | disable}	Enable to query to the FortiGuard Distribution Network (FDN) for FortiGuard Antispam ratings. This option must be enabled for antispam profiles where the FortiGuard Antispam scan is enabled to have an effect.	enable
threshold-ip-connect {1 | 2 | 3}	When you configure the FortiGuard IP reputation check under sender reputation in a session profile, if you select the client connection option, FortiGuard Antispam Service determines if the IP address of the SMTP server is blocklisted during the connection phase. FortiGuard categorizes the blocklisted IP addresses into three levels: level 3 has bad reputation; level 2 has worse reputation; and level 1 has the worst reputation. To avoid false positives, you can specify which level to block. Enter the threshold to block email whose rating is equal to or worse than that level. For example, if you want to block level 1 and level 2 but not level 3, enter 2.	2
url-redirect-lookup {enable | disable}	Enable to connect to web servers in order to resolve URL redirects to their target URLs (for example, a tiny URL that expands to a longer URL). The FortiMail unit can then queriy the FortiGuard AntiSpam database about the target URL — not the redirected URL. **Note:** Your network must allow the FortiMail unit to send HTTP/HTTPS requests to web servers in order to get the destination URL. See also required port numbers in the FortiMail Administration Guide.	enable

Related topics

system fortiguard antivirus update

system fortiguard url-protection

Use this command to configure content disarm and reconstruction (CDR) URL click protection options.

Newsletters often do not embed images in email in order to keep the email file size small so that email can be sent to many people quickly. Instead, the image files are stored at a URL on a web server or CDN. Email clients download and display the image later, when each person reads their email.

Normal HTML email newsletters often include a plain text version or a link to a web page to fall back if the images cannot be displayed in the email. Spammers and malware, however, can abuse requests to the image URLs in order to detect which recipient email addresses are valid, even when SMTP recipient verification is disabled, and to bypass email antispam and antivirus scans by transmitting the content over HTTPS instead of SMTP.

For this reason, like hyperlink URLs, image URLs also have click protection options.

Syntax

```
config system fortiguard url-protection
   set click-action {allow-with-confirmation | block}
   set click-category {all | default | phishing | unrated}
   set isolator-category {all | default | phishing | unrated}
   set isolator-img-src-status {enable | disable}
   set isolator-url-base <fortiisolator_url><FortiIsolator_url>
   set malformed-html-tag-content-action {remove | rewrite}
   set neutralize-category {all | default | phishing | unrated}
   set neutralize-img-src-status {enable | disable}
   set remove-category {all | default | phishing | unrated}
   set remove-img-src-status {enable | disable}
   set rewrite-category {all | default | phishing | unrated}
   set rewrite-img-src-status {enable | disable}
   set rewrite-url-base <FortiMail_url>
   set sandbox-click-action {allow-with-confirmation | block | submit-only}
   set sandbox-status {enable | disable}
   set sandbox-timeout <timeout_int>
   set sandbox-timeout-action {allow | allow-with-confirmation | block}
end
```

Variable	Description	Default
click-action {allow-with-confirmation | block}	Select how the link will behave when click handling applies, and a user clicks a link.	block
click-category {all | default | phishing | unrated}	Select which URL rating category a URL must match in order to receive click handling. For all other URL categories not selected, you can use sandbox-status {enable | disable} to send them to FortiSandbox for more scanning	default

Variable	Description	Default
isolator-category {all | default | phishing | unrated}	Select which URL rating category a URL must match in order to be reached through FortiIsolator.	unrated
isolator-img-src-status {enable | disable}	Enable to use FortiIsolator with the URLs of images that are stored on remote web servers for HTML email.	enable
isolator-url-base <fortiisolator_url><FortiIsolator_url>	Enter the prefix `https://` and then the FQDN or IP address of FortiIsolator. **Note:** The `https://` protocol prefix is required.	
malformed-html-tag-content-action {remove | rewrite}	Select whether to remove or rewrite an HTML tag if it is malformed.	remove
neutralize-category {all | default | phishing | unrated}	Select which URL rating category a URL must match in order to be neutralized.	unrated
neutralize-img-src-status {enable | disable}	Enable to neutralize URLs of images that are stored on remote web servers. **Note:** When you update FortiMail firmware from a previous version, default values are applied to any new settings. If this setting is new, the default results in a change in behavior. If you prefer the previous behavior, then enter: `set neutralize-img-src enable`	disable
remove-category {all | default | phishing | unrated}	Select which URL rating category a URL must match in order to be removed.	default
remove-img-src-status {enable | disable}	Enable to remove the URLs of images that are stored on remote web servers.	enable
rewrite-category {all | default | phishing | unrated}	Select which URL rating category a URL must match in order to be rewritten.	unrated
rewrite-img-src-status {enable | disable}	Enable to rewrite the URLs of images that are stored on remote web servers.	enable

Variable	Description	Default
	Note: When you update FortiMail firmware from a previous version, default values are applied to any new settings. If this setting is new, the default results in a change in behavior. If you prefer the previous behavior, then enable this setting.	
rewrite-url-base <FortiMail_url>	Enter the prefix `https://` and then the FQDN or IP address of FortiMail. When users click a hyperlink, they will be directed to the rewritten URL on FortiMail first. **Note:** The `https://` protocol prefix is required. **Tip:** The URL is rewritten in the format: `https://example.com/fmlurlsvc/?fewReq/baseValue&url=originalUrlEscaped` where `originalUrlEscaped` is the original URL in URL-encoded format. If you want to convert it back to see the original URL, you can use a text editor or online service such as: https://www.urldecoder.org	
sandbox-click-action {allow-with-confirmation | block | submit-only}	Select how the link will behave when a user clicks a link during a FortiSandbox scan: • `allow-with-confirmation`: Allow access with a warning. • `block`: Block access. • `submit-only`: Allows access while sending the URLs for scanning.	allow-with-confirmation
sandbox-status {enable | disable}	For all other URL categories not selected in click-category {all | default | phishing | unrated},enable this setting if you want to send them to FortiSandbox for scanning	disable
sandbox-timeout <timeout_int>	When the URLs are sent to FortiSandbox for scanning, it can take some time to get the results. Enter how long (in seconds) to wait for FortiSandbox scan results. If FortiMail does not get a reply in this time, then click handling instead uses the action specified in sandbox-timeout-action {allow | allow-with-confirmation | block}.	5
sandbox-timeout-action {allow | allow-with-confirmation | block}	Select how the link will behave when a user clicks a link after a FortiSandbox scan timeout (sandbox-timeout <timeout_int>).	allow

Related topics

file content-disarm-reconstruct

profile content

system fortisandbox

The FortiSandbox unit is used for automated sample tracking, or sandboxing. You can send suspicious email attachments to FortiSandbox for inspection when you configure antivirus profiles. If the file exhibits risky behavior, or is found to contain a virus, the result will be sent back to FortiMail and a new virus signature is created and added to the FortiGuard antivirus signature database. For more information about FortiSandbox, please visit Fortinet's web site at https://www.fortinet.com.

Syntax

```
config system fortisandbox
   config file-pattern
      edit <table_value>
         set pattern <string>
      end
   config file-types
      edit {adobe-flash | archive | html | jar | javascript | pdf | msoffice-document | windows-
           executable}
         set status {enable | disable}
      end
   set admin-email <email_str>
   set bypass-one-time-URL {enable | disable}
   set host <hostname_or_ip>
   set max-file-size <integer_value>
   set max-file-size-status {enable | disable}
   set max-URL-per-email
   set scan-mode {scan-and-wait | scan-only}
   set scan-order {antispam-content-sandbox | antispam-sandbox-content | sandbox-antispam-
       content}
   set scan-result-retention
   set scan-timeout
   set service-type {appliance | cloud | cloud-enhanced}
   set statistics-interval <minutes>
   set status {enable | disable}
   set URL-scan-category
   set URL-scan-email-selection
   set URL-scan-on-rating-error {enable | disable}
end
```

Variable	Description	Default
file-pattern	Enter the file patterns to upload to FortiSandbox	
<table_value>	Enter the item number to edit.	
pattern <string>	Enter the pattern value.	
file-types	Enter the file types to upload to FortiSandbox for scanning.	
edit <file_types>	Enter the desired attachment type to include in the FortiSandbox unit's scanning.	

Variable	Description	Default
status {enable | disable}	Enable or disable the selected file type from the FortiSanbox unit's scanning.	
admin-email <email_str>	Enter the administrator's email address to receive reports and notifications.	
bypass-one-time-URL {enable | disable}	Enable to automatically exempt common one-time URLs, such as password reset URLs, from FortiSandbox scanning.	enable
host <hostname_or_ip>	Enter the host name or IP address of the FortiSandbox.	
max-file-size <integer_value>	Enter the maximum size in kilobytes for files uploaded to FortiSandbox.	
max-file-size-status {enable | disable}	Enable or disable the maximum size for files uploaded to FortiSandbox.	
max-URL-per-email	Maximum number of URLs per email to be scanned. If `service-type` is set to `appliance`, the valid range is 1-100. If `service-type` is set to `cloud` or `cloud-enhanced`, the valid range is 1-12.	3
scan-mode {scan-and-wait | scan-only}	`scan-and-wait` means to submit the suspicious email to FortiSandbox and wait for the results. `scan-only` means just to submit the suspicious email without waiting for the results.	scan-and-wait
scan-order {antispam-content-sandbox | antispam-sandbox-content | sandbox-antispam-content}	Set the order of scanners. Sending files to FortiSandbox usually takes more bandwidth and thus it is better to use is as the last resort.	antispam-content-sandbox
scan-result-retention	Scan result retention period in minutes (0 means no retention).	60
scan-timeout	Timeout value before discarding unfinished scan tasks.	30
service-type {appliance | cloud | cloud-enhanced}	Use either FortiSandbox appliance, FortiSandbox regular cloud service, or FortiSandbox enhanced cloud service. The enhanced cloud service provides a dedicated service for faster performance.	appliance
statistics-interval <minutes>	Specify how long in minutes FortiMail should wait to retrieve some high level statistics from FortiSandbox. The statistics include how much malware is detected and how many files are clean among all the files submitted. Set the value between 1 to 30.	5
status {enable | disable}	Either enable or disable the usage of the unit.	disable
URL-scan-category	Category of the URL to be scanned:	unrated

Variable	Description	Default
	• Security-Risk • all • default • phishing • unrated	
URL-scan-email-selection	Selection of email for URL scan.	
URL-scan-on-rating-error {enable | disable}	Sometimes, FortiMail may not be able to get results from the FortiGuard queries (for example, ratings errors due to network connection failures). In this case, you can choose whether to upload the those URLs to FortiSandbox for scanning. Choosing not to upload those URLs may help improving the FortiSandbox performance.	disable

system geoip-override

Use this command to configure GeoIP lookup overrides.

GeoIP looks up the IP addresses associated with geographic locations in the GeoIP database. However, in some cases, the lookup might not be accurate, such as when clients use a proxy or VPN. You can override the GeoIP lookup result by manually specifying the geographic locations of some IP addresses and ranges.

Only IPv4 addresses are supported for GeoIP overrides.

Syntax

```
config system geoip-override
   edit <profile_name>
      [set description "<description_str>"]
      config ip-ranges
         edit <host_ipv4/mask>
            [set comment "<comment_str>"]
      end
   next
end
```

Variable	Description	Default
<profile_name>	Enter a unique name.	
comment "<comment_str>"	Enter a description or comment.	

Variable	Description	Default
description "<description_str>"	Enter a description or comment.	
<host_ipv4/mask>	Enterthe IPv4 address range or subnet that you want to include in the override.	

Related topics

profile geoip-group

policy access-control delivery

policy access-control receive

policy ip

system global

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

Syntax

```
config system global
   set admin-idle-timeout <timeout_int>
   set admin-lockout-duration <timeout_int>
   set admin-lockout-threshold <attempts_int>
   set admin-maintainer {enable | disable}
   set default-certificate <name_str>
   set dh-params <bits_int>
   set disclaimer-per-domain {enable | disable}
   set disk-monitor {enable | disable}
   set email-migration-status {enable | disable}
   set hostname <host_str>
   set hsts-max-age <days_int>
   set iscsi-initiator-name <name_str>
   set lcd-pin <pin_int>
   set lcd-protection {enable | disable}
   set ldap-server-sys-status {enable | disable}
   set ldap-sess-cache-state {enable | disable}
   set local-domain-name <name_str>
   set mailstat-service {enable | disable}
   set max-admin-per-domain <administrators_int>
   set mta-adv-ctrl-status {enable | disable}
   set operation-mode {gateway | server | transparent}
   set pki-certificate-req {yes | no}
   set pki-mode {enable | disable}
   set port-http <port_int>
```

```
    set port-https <port_int>
    set port-ssh <port_int>
    set port-telnet <port_int>
    set post-login-banner {admin ibe webmail}
    set pre-login-banner {admin}
    set ssl-versions {ssl3 tls1_0 tls1_1 tls1_2 tls1_3}
    set strong-crypto {enable | disable}
    set tftp {enable | disable}
end
```

Variable	Description	Default
admin-idle-timeout <timeout_int>	Enter the amount of time in minutes after which an idle administrative session will be automatically logged out. The maximum idle time out is 480 minutes (eight hours). To improve security, do not increase the idle timeout.	5
admin-lockout-duration <timeout_int>	Enter the lockout duration in minutes after the failed login threshold is reached.	3
admin-lockout-threshold <attempts_int>	Enter the number of failed login attempts before being locked out.	4
admin-maintainer {enable | disable}	Enable or disable the maintainer administrator login. When enabled, the maintainer account can be used to log in from the console after a hard reboot. The password is `\'bcpb\'` followed by the unit serial number. **Caution:** There is a limited time to complete this login. If you try to disable `admin-maintainer`, a message appears warning that the password recovery mechanism will be lost. Do not disable this option if you do not have a backup plan for recovery.	enable
default-certificate <name_str>	Enter the name of a local certificate to use it as the “default" (that is, currently chosen for use) certificate. FortiMail units require a local certificate that it can present to identify itself when clients request secure connections.	factory
dh-params <bits_int>	Enter the minimum size of the Diffie-Hellman prime number for secure connections such as SSH, SMTPS, and HTTPS. Larger bit sizes are slower to generate, but generally more secure. Alternatively, you can set the Diffie-Hellman bit size for individual protocols. See system security crypto on page 342.	2048
disclaimer-per-domain {enable | disable}	Enable to allow individualized disclaimer messages to be configured for each protected domain. Also configure disclaimer-status {disabled | use-domain-setting | use-system-setting} on page 90.	disable
disk-monitor {enable | disable}	Enable to monitor the hard disk status of the FortiMail unit. If a problem is found, FortiMail sends an alert email to the administrator.	disable
email-migration-status {enable | disable}	Enable the email migration from external server.	disable

Variable	Description	Default
hostname <host_str>	Enter the host name of the FortiMail unit.	Varies by model.
hsts-max-age <days_int>	Enter the expiry age for HTTP Strict Transport Security (HSTS) header in HTTPS connections to the GUI. Enter `0` to disable expiry.	365
iscsi-initiator-name <name_str>	Enter the FortiMail iSCSI client name used to communicate with the iSCSI server for centralized quarantine storage. This is only used to change the name generated by the FortiMail unit automatically.	
lcd-pin <pin_int>	Enter the 6-digit personal identification number (PIN) that administrators must enter in order to access the FortiMail LCD panel. The PIN is used only when `lcdprotection` is `enable`.	Encoded value varies.
lcd-protection {enable | disable}	Enable to require that administrators enter a PIN in order to use the buttons on the front LCD panel. Also configure `lcdpin`.	disable
ldap-server-sys-status {enable | disable}	Enable or disable the LDAP server for serving organizational information.	enable
ldap-sess-cache-state {enable | disable}	Enable to keep the continuity of the connection sessions to the LDAP server. Repeated session connections waste network resources.	enable
local-domain-name <name_str>	Enter the local domain name of the FortiMail unit.	
mailstat-service {enable | disable}	Enable the mail statistic service. After you enable this service, a new tab called *Top User Statistics* will appear under *FortiView* on the GUI.	disable
max-admin-per-domain <administrators_int>	Enter the maximum number of administrators per domain. The valid range is 1 to 10.	3
mta-adv-ctrl-status {enable | disable}	Enable to configure advanced session-specific MTA settings (see profile session on page 247) and overwrite the global settings configured elsewhere. **Note:** The MTA advanced control feature is license based. If you do not purchase the advanced management license, this feature is not available.	enable
operation-mode {gateway | server | transparent}	Select the operation mode: • `gateway`: The FortiMail unit acts as an SMTP gateway or MTA, but does not host email accounts. • `server`: The FortiMail unit acts as a standalone email server that hosts email accounts and acts as an MTA. • `transparent`: The FortiMail unit acts as an SMTP proxy. **Note:** Only administrators with `super_admin` privileges may change the FortiMail unit's operation mode.	gateway

Variable	Description	Default
pki-certificate-req {yes | no}	If the administrator's web browser does not provide a valid personal certificate for PKI authentication, the FortiMail unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enter `yes`. To allow password-style fallback, enter `no`.	no
pki-mode {enable | disable}	Enable to allow PKI authentication for FortiMail administrators. See also user pki on page 362 and system admin on page 275. Also configure pki-certificate-req {yes | no}. **Caution:**: Before you disable PKI authentication, enable another mode of authentication for FortiMail administrators and email users that are currently using PKI authentication. If you don't, they will not be able to log in.	disable
port-http <port_int>	Enter the HTTP port number for administrative access on all interfaces.	80
port-https <port_int>	Enter the HTTPS port number for administrative access on all interfaces.	443
port-ssh <port_int>	Enter the SSH port number for administrative access on all interfaces.	22
port-telnet <port_int>	Enter the Telnet port number for administrative access on all interfaces.	23
post-login-banner {admin ibe webmail}	Select which login pages will display the legal disclaimer: • `admin`: Select to display the disclaimer message **after** the administrator logs into the FortiMail administrative GUI. • `webmail`: Select to display the disclaimer message after the user logs into FortiMail webmail. • `ibe`: Select to display the disclaimer message after the user logs into the FortiMail unit to view IBE encrypted email.	admin
pre-login-banner {admin}	Enable or disable the legal disclaimer **before** the administrator logs into the FortiMail GUI.	admin
ssl-versions {ssl3 tls1_0 tls1_1 tls1_2 tls1_3}	Select which SSL/TLS version(s) FortiMail will accept in secure connections: • from clients (HTTPS web browsers and SMTPS mail clients) • to servers (protected mail servers and Syslog with TCP over TLS) Separate multiple versions with a space. Alternatively, for some protocols, you can individually specify which SSL/TLS versions FortiMail accepts. See system security crypto on page 342. **Note:** The `ssl3` option is not available if strong-crypto {enable | disable} is enabled. **Note:** Some old versions of web browsers, email clients (for example, Microsoft Outlook 2007 and older), and MTAs may only support TLS 1.0. Therefore they cannot connect to FortiMail if you enable strong-crypto {enable | disable} and/or disable TLS 1.0.	tls1_1 tls1_2 tls1_3

Variable	Description	Default
strong-crypto {enable | disable}	Enable to use strong encryption and only allow strong ciphers (AES-128 or better) and digest (SHA-256 or better) for HTTPS, SSH, and Syslog with TCP over TLS. Old SSL/TLS versions with known vulnerabilities such as SSL 3.0 are also disabled, so this setting may partially override ssl-versions {ssl3 tls1_0 tls1_1 tls1_2 tls1_3}. Alternatively, for some protocols, you can individually specify which cipher suites FortiMail accepts for each protocol. See system security crypto on page 342. **Note:** Old mail clients and old browser versions such as Microsoft Internet Explorer 6.0 do not support strong encryption.	disable
tftp {enable | disable}	Enable to allow use of TFTP in FIPS mode.	enable

Related topics

- domain-setting
- system interface
- profile encryption
- system security crypto

system ha

Use this command to configure the FortiMail unit to work in an high availability (HA) cluster or to put the cluster in an HA group in order to increase processing capacity or availability.

Alternatively, to automatically configure most HA settings on secondary units, you can instead use `exec ha hb join`.

For deployment topology diagrams and other details, see the FortiMail Administration Guide.

Syntax

```
config system ha
   set state {enable | disable}
   set type {group | member}
   set mode {active-active | active-passive}
   set password "<password_str>"
   set hb-base-port <port_int>
   set hb-lost-threshold <seconds_int>
   set remote-services-as-heartbeat {enable | disable}
   set mail-data-sync {enable | disable}
   set mailqueue-data-sync {enable | disable}
   set cluster-id <name_str>
```

```
config group
   edit <group_name>
      [set comment "<comment_str>"]
      set mode {active-active | active-passive}
      set role {primary | secondary}
      set primary-backup {enable | disable}
   next
end
config member
   edit <member_name>
      [set comment "<comment_str>"]
      set role {primary | secondary}
      set primary-backup {enable | disable}
      set ip <interface_ipv4mask>
      set ipv6 <interface_ipv6mask>
      set hostname <hostname_str>
      set group <group_name>
   next
end
config interface
   edit <interface_name>
      set heartbeat-status {enable | disable}
      set port-monitor {enable | disable}
      set add-to-bridge {enable | disable}
      set virtual-ip <vip_ipv4/mask>
      set virtual-ip6 <vip_ipv6mask>
      set virtual-hostname <hostname_str>
   next
end
config service
   edit local-hd
      set status {enable | disable}
      set check-interval <seconds_int>
      set retries <retries_int>
   edit local-ports
      set check-interval <seconds_int>
      set retries <retries_int>
   next
   edit remote-http
      set status {enable | disable}
      set check-interval <seconds_int>
      set check-timeout <seconds_int>
      set retries <retries_int>
      set port <port-number_int>
      set hostname <hostname_str>
   next
   edit remote-imap
      set status {enable | disable}
      set check-interval <seconds_int>
      set check-timeout <seconds_int>
      set retries <retries_int>
      set port <port-number_int>
      set hostname <hostname_str>
   next
   edit remote-pop
      set status {enable | disable}
      set check-interval <seconds_int>
```

```
            set check-timeout <seconds_int>
            set retries <retries_int>
            set port <port-number_int>
            set hostname <hostname_str>
        next
        edit remote-smtp
            set status {enable | disable}
            set check-interval <seconds_int>
            set check-timeout <seconds_int>
            set retries <retries_int>
            set port <port-number_int>
            set hostname <hostname_str>
        next
    end
    set action-on-failure {off | become-secondary | restore-role}
end
```

Variable	Description	Default
<group_name>	Enter the name for the HA cluster. Group HA settings are used only if type {group | member} is group.	
<interface_name>	Enter the name of the network interface.	
<member_name>	Enter the name for the FortiMail unit in the HA cluster. By default, the first entry's name is the hostname of this FortiMail unit.	
action-on-failure {off | become-secondary | restore-role}	Select what the primary unit will do after it fails (if it can recover), either: • off — Do not automatically rejoin the HA cluster. To manually rejoin it to the cluster, manually select the effective role (exec ha restore). • become-secondary — Automatically rejoin the cluster, but the effective role becomes secondary. To restore it to acting as primary, manually select the effective role (exec ha restore). **Tip:** In most cases, you should select become-secondary. • restore-role — Automatically rejoin the cluster, but the effective role becomes primary again.The secondary unit that was temporarily acting as primary also automatically becomes secondary again. This option may be useful if the cause of failure is temporary and rare, but may cause problems if the cause of failure is recurring, resulting in many extra role changes. This setting applies only if role {primary | secondary} is primary. See also the HA mode details and examples in the FortiMail Administration Guide.	
add-to-bridge {enable | disable}	Enable to include the network interface in the bridge. This setting is available only if operation-mode {gateway | server | transparent} is transparent, and if there is no virtual-ip <vip_ipv4/mask> already on the network interface.	disable
check-interval <seconds_int>	Enter the amount of time in seconds between each try.	120

Variable	Description	Default
check-timeout <seconds_int>	Enter the amount of time in seconds to wait for a response when service monitoring tries to connect.	30
cluster-id <name_str>	Enter the name of the HA cluster to identify its log messages when multiple clusters send their logs to the same FortiAnalyzer unit.	
comment "<comment_str>"	Enter a comment or description.	
group <group_name>	Select which HA group to join. This setting is available only if type {group | member} is `group`.	
hb-base-port <port_int>	Enter the first of multiple port numbers (see required TCP/UDP open port numbers in the FortiMail Administration Guide) that will be used for: • heartbeat signals • synchronization control • data synchronization • configuration synchronization **Note:**In addition to a lost heartbeat, other unresponsive network services and hardware failure can also be used to trigger failover. See config service on page 316 and the HA heartbeat and synchronization details in the FortiMail Administration Guide.	20000
hb-lost-threshold <seconds_int>	Enter the amount of time, in seconds, that a primary unit can be unresponsive until HA detects a failure and performs the action in action-on-failure {off | become-secondary | restore-role}. **Caution:** If you have service level agreements (SLA), then you may be required to keep this time short. If the failure detection time is too long, email delivery could be delayed or fail until HA detects the failure. This reduces service uptime. **Tip:** To determine the best heartbeat threshold, monitor your FortiMail unit's performance. Examine how long each high system resource usage lasts. Configure a threshold that is longer than most peak usage. This gives the secondary unit enough time to accurately confirm unresponsiveness, and avoid unnecessary failovers. (Heartbeat responses may be slow during peak load.) To monitor performance, you can use the dashboard in the GUI, system ha, or the CLI: `diagnose sys top delay 1 lines 10`	120
heartbeat-status {enable | disable}	Enable if this network interface will listen for HA heartbeat and synchronization communications. **Note:** You must enable this option on at least one of the heartbeat interfaces that you defined for the unit in ip <interface_ipv4mask> and/or ipv6 <interface_ipv6mask> . Otherwise HA will detect a failure.	disable

Variable	Description	Default
	Note:Don't disconnect the heartbeat link once HA is enabled. If the heartbeat is accidentally interrupted for active-passive HA mode, such as when a network cable is temporarily disconnected, the secondary unit will assume that the primary unit has failed, and become the new primary unit. If no failure has actually occurred, both FortiMail units will be operating as primary units at the same time. This can cause an IP address conflict. In active-active HA, this can disrupt configuration synchronization. **Tip:** For better heartbeat reliability, create two heartbeat links: a primary and a secondary. Directly link the pair of heartbeat ports with an Ethernet crossover cable, or connect them through a dedicated local switch that is not connected to your overall network. This ensures enough bandwidth and low latency for the synchronization and heartbeat. If the heartbeat is interrupted, then a failover may occur. See the HA heartbeat and synchronization details in the FortiMail Administration Guide.	
hostname <hostname_str>	Enter the hostname of the network interface that will listen for the heartbeat and synchronization. Alternatively, to define a heartbeat interface, instead use ipv6 <interface_ipv6mask> or ip <interface_ipv4mask>. **Note:** You must also bring up and then enable heartbeat-status {enable | disable} on the interface. If it is disabled, but the hostname is configured here, then HA will detect that the heartbeat link has failed. **Tip:** Use a hostname to define the heartbeat interface (not an IP address) in environments where IP addresses change often, such as with VMs and containers. Heartbeat hostnames might **not** be the same as the SMTP relay/proxy hostname (hostname <host_str> in mail settings) and virtual hostname for active-passive HA (virtual-hostname <hostname_str>).	
ip <interface_ipv4mask>	Enter the IP address of the network interface that will listen for the heartbeat and synchronization. Alternatively, to define a heartbeat interface, instead use ipv6 <interface_ipv6mask> or hostname <hostname_str>. **Note:** You must also bring up and then enable heartbeat-status {enable | disable} on the interface. If it is disabled, but the IP address is configured here, then HA will detect that the heartbeat link has failed. **Tip: Don't use DHCP IP addresses for heartbeat links.** This can disrupt the heartbeat when an IP address has not been assigned yet by the DHCP server, such as during firmware upgrades, if there is an IP address conflict, or if a DHCP reservation fails. Use static IP addresses instead.	
ipv6 <interface_ipv6mask>	Enter the IP address of the network interface that will listen for the heartbeat and synchronization. Alternatively, to define a heartbeat interface, instead use ip <interface_ipv4mask> or hostname <hostname_str>.	

Variable	Description	Default
	Note: You must also bring up and then enable heartbeat-status {enable | disable} on the interface. If it is disabled, but the IP address is configured here, then HA will detect that the heartbeat link has failed. **Tip: Don't use DHCP IP addresses for heartbeat links.** This can disrupt the heartbeat when an IP address has not been assigned yet by the DHCP server, such as during firmware upgrades, if there is an IP address conflict, or if a DHCP reservation fails. Use static IP addresses instead.	
mail-data-sync {enable | disable}	Enable if the HA cluster does not store its mail data on a NAS server, and you need to use HA communications to synchronize its system quarantine, per-recipient quarantines, email archives, email users' preferences, and (server mode only) mailboxes. This setting applies only if mode {active-active | active-passive} is `active-passive`. **Tip:** You can manually initiate a data synchronization whenever significant changes occur (`exec ha sync command config-sync-start`).	enable
mailqueue-data-sync {enable | disable}	Enable if you want to synchronize the mail queue with FortiMail units in the HA cluster. This setting applies only if mode {active-active | active-passive} is `active-passive`. **Caution:** If the primary unit experiences a hardware failure and you cannot restart it, and if this option is disabled, MTA queue directory data could be lost. **Note:** If you enable this option, it can reduce performance, and is not guaranteed to prevent data loss. Mail queue directories are very dynamic. Many email could be added to the queue between each sync. If you disable this option, data loss might not occur, either. After a failover, when the unit rejoins the cluster, a separate synchronization mechanism occurs. This often restores the mail queue. For details, see HA synchronization details in the FortiMail Administration Guide.	disable
mode {active-active | active-passive}	Select the HA operating mode, either: • `active-active` — All FortiMail units in the HA cluster process email. This increases throughput when more units join. However if any of the units fail, there may be data loss. • `active-passive` — Only the primary FortiMail unit processes email, while other units stand by and keep in sync. This avoids data loss if any of the units fail. However there is no increased throughput when more units join. See also the HA mode details and examples in the FortiMail Administration Guide.	off
password "<password_str>"	Enter a password for this HA cluster. Before FortiMail units in the HA cluster synchronize with each other, they verify that they have the same password. This prevents them from accidentally synchronizing with the wrong cluster. Therefore you must enter the same HA password on all of them.	

Variable	Description	Default
port <port-number_int>	Enter the listening port number of the service on the primary unit and (active-active HA only) secondary. See also required TCP/UDP open port numbers in the FortiMail Administration Guide.	Varies by service (25 for SMTP etc.)

port-monitor {enable | disable}	Enable to monitor the network interface for failure. If it fails, a failover occurs.
	Also configure settings in:
	`config service`
	`edit local-ports`
		disable

primary-backup {enable | disable}	If mode {active-active | active-passive} is `active-active`, then there can be many secondary units. If role {primary | secondary} is `secondary`, and you want the unit to become the new primary when a failure is detected, enable this setting. **Note:** Usually you should have a primary backup. Otherwise configuration synchronization will be interrupted upon failure. See HA heartbeat and synchronization details in the Administration Guide.	disable

remote-services-as-heartbeat {enable | disable}	Enable to avoid the action in action-on-failure {off | become-secondary | restore-role} if the heartbeat links (see heartbeat-status {enable | disable}) temporarily fail, but service monitoring detects that the primary unit is still available.
	Also configure settings in:
	`config service`
	`edit remote-smtp`
	`edit remote-http`
	`edit remote-imap`
	`edit remote-pop`
		disable

retries <retries_int>	Enter the number of consecutive unsuccessful tries that indicates a failure.	3
role {primary | secondary}	Select the role of the FortiMail unit in the HA group. Each FortiMail unit's role in the HA cluster is not synchronized because this distinguishes the primary and secondary units. Effects of the role vary by mode {active-active | active-passive}.	primary
state {enable | disable}	Enable or disable this FortiMail unit to operate as part of an HA cluster.	disable
status {enable | disable}	Enable or disable service monitoring. **Note:** This setting does not exist for network interfaces. Instead use port-monitor {enable | disable}.	disable
type {group | member}	Select the type of HA deployment, either: • `member` — Multiple FortiMail units work together in one HA pair or cluster. • `group` — Multiple HA clusters work together in an HA group. For example, if you have one data center to protect, you only need one cluster. However if you have two data centers for geographic redundancy, then you can join the clusters together to form an HA group.	member

Variable	Description	Default
	Depending on your throughput or failover requirements, with group HA, you can mix the HA modes. Each cluster in an HA group has its own HA mode. At the HA group level, there is also an HA mode that defines throughput or failover amongst the clusters.	
virtual-ip <vip_ipv4/mask>	Enter a virtual IP address and netmask that the primary unit will have on this network interface. Upon failure detection, the secondary will become the new primary and start to use the virtual IP address. For gateway mode and server mode deployments, DNS records should be configured to point to the virtual IP address, not physical IP addresses.See also system interface on page 322, and the HA mode details and examples in the FortiMail Administration Guide. This setting is available only if mode {active-active | active-passive} is `active-passive`.	
virtual-ip6 <vip_ipv6mask>	Enter the virtual IPv6 address and netmask for this interface. This setting is available only if mode {active-active | active-passive} is `active-passive`.	
virtual-hostname <hostname_str>	Enter a virtual hostname. Similar to behavior with virtual-ip <vip_ipv4/mask>, the virtual hostname belongs to the current primary unit. Upon failover, the secondary unit becomes the new primary unit, and so it starts to use the virtual hostname instead. This setting is available only if mode {active-active | active-passive} is `active-passive`.	

Related topics

- mailsetting storage config
- ha hb join
- ha failover
- ha restore
- ha-group failover
- ha-group restore

system interface

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

Proxy and built-in MTA behaviors are configured separately based upon whether the SMTP connection is considered to be incoming or outgoing. Because a network connection considers the network layer rather than the application layer when deciding whether to intercept a connection, the concept of incoming and outgoing

connections is based upon slightly different things than that of incoming and outgoing email messages: directionality is determined by IP addresses of connecting clients and servers, rather than the email addresses of recipients.

- **Incoming connections** are destined for the SMTP servers that are protected domains of the FortiMail unit. For example, if the FortiMail unit is configured to protect the SMTP server whose IP address is 10.1.1.1, the FortiMail unit treats all SMTP connections destined for 10.1.1.1 as incoming. For information about configuring protected domains, see domain-setting on page 88.
- **Outgoing connections** are destined for SMTP servers that the FortiMail unit has not been configured to protect. For example, if the FortiMail unit is **not** configured to protect the SMTP server whose IP address is 192.168.1.1, all SMTP connections destined for 192.168.1.1 will be treated as outgoing, regardless of their origin.

Syntax

```
config system interface
   edit {<physical_interface_name> | <logical_interface_name> | loopback
      set allowaccess {ping http https snmp ssh telnet}
      set connection {enable | disable}
      set defaultgw {enable | disable}
      set bridge-member {enable | disable}
      set ip <ipv4mask>
      set ip6 <ipv6mask>
      set mac-addr <xx.xx.xx.xx.xx.xx>
      set mailaccess {imap | imaps | pop3 | pop3s | smtp | smtps}
      set mode {static | dhcp}
      set mtu <mtu_int>
      set proxy-smtp-in-mode {pass-through | drop | proxy}
      set proxy-smtp-local status {enable | disable}
      set proxy-smtp-out-mode {pass-through | drop | proxy}
      set speed {auto | 10full | 10half | 100full | 100half | 1000full}
      set status {down | up}
      set type {vlan | redundant}
      set vlanid <vlan_int>
      set webaccess {enable | disable}
      set redundant-link-monitor {mii-link | arp-link}
      set redundant-arp-ip <ip_addr>
      set redundant-member <member_interface_name>
end
```

Variable	Description	Default
<physical_interface_name>	Enter the name of the physical network interface, such as port1.	
<logical_interface_name>	Enter a name for the VLAN or redundant interface. Then set the interface type.	
loopback	A loopback interface is a logical interface that is always up (no physical link dependency) and the attached subnet is always present in the routing table.	

Variable	Description	Default
	The FortiMail unit's loopback IP address does not depend on one specific external port, and is therefore possible to access through several physical or VLAN interfaces. You can only add one loopback interface on the FortiMail unit. The loopback interface is useful when you use a Layer 2 load balancer in front of several FortiMail units. In this case, you can set the FortiMail loopback interface's IP address the same as the load balancer's IP address and thus the FortiMail unit can pick up the traffic forwarded to it from the load balancer.	
allowaccess {ping http https snmp ssh telnet}	Enter one or more of the following protocols to add them to the list of protocols permitted to administratively access the FortiMail unit through this network interface: • `ping`: Allow ICMP ping responses from this network interface. • `http`: Allow HTTP access to the GUI, webmail, and per-recipient quarantines. See also https-redirect-status {enable | disable}. **Caution**: HTTP connections are **not** secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail unit, enable this option only on network interfaces connected directly to your management computer. • `https`: Allow secure HTTP (HTTPS) access to the GUI, webmail, per-recipient quarantines, and REST API. See also system web-service on page 353. • `snmp`: Allow SNMP v2 access. For more information, see system snmp community on page 344, system snmp sysinfo on page 345, and system snmp threshold on page 346. • `ssh`: Allow SSH access to the CLI. • `telnet`: Allow Telnet access to the CLI. **Caution:** Telnet connections are **not** secure and can be intercepted by a third party. To reduce risk to the security of your FortiMail unit, enable this option only on network interfaces connected directly to your management computer. For related settings such as listening port numbers for each service, see also system global on page 311. To control SMTP access, configure access control rules and session profiles. For details, see cloud-api profile antivirus on page 76 and profile session on page 247.	Varies by network interface.
connection {enable | disable}	Enable for the FortiMail unit to attempt to obtain DHCP addressing information from the DHCP server. Disable this option if you are configuring the network interface offline, and do not want the unit to attempt to obtain addressing information at this time. **Note**: This command is only available when mode {static | dhcp} is `dhcp`.	disable
defaultgw {enable | disable}	Enable to retrieve both the default gateway and DNS addresses from the DHCP server, replacing any manually configured values.	disable

Variable	Description	Default
	Note: This command is only available when mode {static | dhcp} is `dhcp`.	
bridge-member {enable | disable}	Enable to bridge the port to the management IP. See Editing network interfaces for information on bridged networks in transparent mode. Bridging is the default configuration for network interfaces when the FortiMail unit operates in transparent mode, and the FortiMail unit will bridge all connections occurring through it from the network to the protected email servers. In cases where the email servers that are protected by the FortiMail unit are located on different subnets, you must connect those email servers through separate physical ports on the FortiMail unit, and configure the network interfaces associated with those ports, assigning IP addresses and removing them from the bridge. **Note**: This command is only available when operation-mode {gateway | server | transparent} is `transparent`, and only for non-management ports.	enable
ip <ipv4mask>	Enter the IP address and netmask of the network interface. If the FortiMail unit is in transparent mode, ***IP***/***Netmask*** may alternatively display ***bridging***. This means that the network interface is acting as a Layer 2 bridge. If high availability (HA) is also enabled, ***IP*** and ***Netmask*** may alternatively display ***bridged (isolated)*** while the effective operating mode is ***secondary*** and therefore the network interface is currently disconnected from the network, or ***bridging (waiting for recovery)*** while the effective operating mode is ***failed*** and the network interface is currently disconnected from the network but a failover may soon occur, beginning connectivity.	
ip6 <ipv6mask>	Enter the IPv6 address and netmask of the network interface. If the FortiMail unit is in transparent mode, ***IP***/***Netmask*** may alternatively display ***bridging***. This means that the network interface is acting as a Layer 2 bridge. If high availability (HA) is also enabled, ***IP*** and ***Netmask*** may alternatively display ***bridged (isolated)*** while the effective operating mode is ***secondary*** and therefore the network interface is currently disconnected from the network, or ***bridging (waiting for recovery)*** while the effective operating mode is ***failed*** and the network interface is currently disconnected from the network but a failover may soon occur, beginning connectivity.	
mac-addr <xx.xx.xx.xx.xx.xx>	Enter a MAC address to override the factory set MAC address of this interface.	Factory set
mailaccess {imap | imaps | pop3 | pop3s | smtp | smtps}	Select which types of mail access to allow on the interface.	
mode {static | dhcp}	Enter the interface mode. If configuring for DHCP, see connection {enable | disable} and defaultgw {enable | disable}.	static

Variable	Description	Default
	DHCP mode applies only if the FortiMail unit is operating in gateway mode or server mode.	
mtu <mtu_int>	Enter the maximum packet or Ethernet frame size in bytes. If network devices between the FortiMail unit and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance. The valid range is from 576 to 1500 bytes.	1500
proxy-smtp-in-mode {pass-through | drop | proxy}	Enter how the proxy or built-in MTA will handle SMTP connections on each network interface that are **incoming** to the IP addresses of email servers belonging to a protected domain: • `pass-through`: Permit but do not proxy or relay. Because traffic is not proxied or relayed, no policies will be applied. • `drop`: Drop the connection. • `proxy`: Proxy or relay the connection. Once intercepted, policies determine any further scanning or logging actions. For more information, see policy ip, policy recipient on page 156, and config policy recipient on page 101. **Note:** Depending on your network topology, you may want to verify that email is not being scanned twice. This could result if, due to mail routing, an email would travel through the FortiMail unit multiple times in order to reach its final destination, and you have entered `proxy` more than once for each interface and/or directionality. For an example, see the FortiMail Administration Guide. This option is only available if operation-mode {gateway | server | transparent} is `transparent`.	proxy
proxy-smtp-local status {enable | disable}	Enable to allow connections destined for the FortiMail unit itself. This option is only available if operation-mode {gateway | server | transparent} is `transparent`.	disable
proxy-smtp-out-mode {pass-through | drop | proxy}	Enter how the proxy or built-in MTA will handle SMTP connections on each network interface that are incoming to the IP addresses of email servers belonging to a protected domain: • `pass-through`: Permit but do not proxy or relay. Because traffic is not proxied or relayed, no policies will be applied. • `drop`: Drop connections. • `proxy`: Proxy or relay connections. Once intercepted, policies determine any further scanning or logging actions. For more information, see policy delivery-control on page 149.	pass-through

Variable	Description	Default
	Note: Depending on your network topology, you may want to verify that email is not being scanned twice. This could result if, due to mail routing, an email would travel through the FortiMail unit multiple times in order to reach its final destination, and you have entered `proxy` more than once for each interface and/or directionality. For an example, see the FortiMail Administration Guide. This option is only available if operation-mode {gateway | server | transparent} is `transparent`.	
redundant-arp-ip <ip_addr>	Enter the redundant interface ARP monitoring IP target. This option is only available when redundant-link-monitor {mii-link | arp-link} is `arp-link`.	
type {vlan | redundant}	• `vlan`: A virtual LAN (VLAN) subinterface, is a virtual interface on a physical interface. The subinterface allows routing of VLAN tagged packets using that physical interface, but it is separate from any other traffic on the physical interface. Virtual LANs (VLANs) use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security. One example of an application of VLANs is a company's accounting department. Accounting computers may be located at both main and branch offices. However, accounting computers need to communicate with each other frequently and require increased security. VLANs allow the accounting network traffic to be sent only to accounting computers and to connect accounting computers in different locations as if they were on the same physical subnet. Also configure redundant-link-monitor {mii-link | arp-link} and redundant-member <member_interface_name>. • `redundant`: On the FortiMail unit, you can combine two or more physical interfaces to provide link redundancy. This feature allows you to connect to two or more switches to ensure connectivity in the event one physical interface or the equipment on that interface fails. In a redundant interface, traffic is only going over one interface at any time. This differs from an aggregated interface where traffic is going over all interfaces for increased bandwidth. This difference means redundant interfaces can have more robust configurations with fewer possible points of failure. This is important in a fully-meshed HA configuration. Also configure vlanid <vlan_int>.	
redundant-link-monitor {mii-link | arp-link}	Select the parameters to monitor the connections of the redundant interfaces. • `mii-link`: Media Independent Interface is an abstract layer between the operating system and the NIC which detects whether the failover link is running.	mii-link

Variable	Description	Default
	• `arp-link`: Address Resolution Protocol periodically checks whether the remote interface is reachable. Also configure redundant-arp-ip <ip_addr>. This option is only available when type {vlan | redundant} is `redundant`.	
redundant-member <member_interface_name>	Enter the redundant member for interface failover. This option is only available when type {vlan | redundant} is `redundant`.	
vlanid <vlan_int>	Enter the VLAN ID for logically separating devices on a network into smaller broadcast domains. This option is only available when type {vlan | redundant} is `vlan`.	
webaccess {enable | disable}	Allow web access with the interface.	
speed {auto | 10full | 10half | 100full | 100half | 1000full}	Enter the speed of the network interface. **Note**: Some network interfaces may not support all speeds.	auto
status {down | up}	Enter either `up` to enable the network interface to send and receive traffic, or `down` to disable the network interface.	up

Related topics

sensitive data

system admin

system link-monitor

Use this command to propagate status of a sort to other ports.

Syntax

```
config system link-monitor
   set link-monitor-delay
   set link-monitor-interval
   set link-monitor-status {enable | disable}
end
```

Variable	Description	Default
link-monitor-delay	Enter in seconds the amount of time to delay after link state changes.	

Variable	Description	Default
link-monitor-interval	Enter in seconds the time the link monitor will perform an interval check.	
link-monitor-status {enable | disable}	Enable the link monitor.	8

system mailserver

Use this command to configure system-wide mail settings.

Syntax

```
config system mailserver
   config mail-queue
      edit {default | incoming | outgoing}
         set queue-timeout <hours_int>
         set queue-dsn-timeout <days_int>
         set queue-warning <hours_int>
         set queue-retry <minutes_int>
         set queue-max-delivery-attempt <tries_int>
         set queue-max-delivery-attempt-on-dsn <tries_int>
      end
   set queue-regular-delivery-attempt <tries_int>
   set deadmail-expiry <days_int>
   set default-auth-domain <domain_name>
   set defer-delivery-starttime <time_str>
   set defer-delivery-stoptime <time_str>
   set delivery-esmtp {no | yes}
   set delivery-failure-conditions {dns-failure | mta-failure-permanant | mta-failure-temporary |
        network-failure-connection | network-failure-other}
   set delivery-failure-handling-option {normal | relay-to-host}
   set delivery-failure-host <host_name>
   set delivery-failure-min-age <minutes_int>
   set delivery-tracking-status {enable | disable}
   set dsn-ehlo-option {host-name | domain-name | other-name}
   set dsn-ehlo-other-name <name_str>
   set dsn-email-attach-orig {enable | disable}
   set dsn-email-customization-status {enable | disable}
   set dsn-sender-address <email_str>
   set dsn-sender-displayname <name_str>
   set dsn-status {enable | disable}
   set imap-service {enable | disable}
   set ip-pool-direction {all | exclude-internal-to-internal}
   set ldap-domaincheck {enable | disable}
   set ldap-domaincheck-auto-associate {enable | disable}
   set ldap-domaincheck-internal-domain <domain_str>
   set ldap-domaincheck-profile <profile_str>
   set local-domain-name <local-domain_str>
```

```
    set pop3-port <port_int>
    set pop3-service {enable | disable}
    set relay-server-name <relay_name>
    set relay-server-status {enable |disable}
    set show-accept-cert-ca {enable | disable}
    set smtp-auth {enable | disable}
    set smtp-auth-over-tls {enable | disable}
    set smtp-auth-smtps {enable | disable}
    set smtp-delivery-addr-pref {ipv4-ipv6 | ipv6-ipv4 | ipv4 | ipv6}
    set smtp-delivery-session-preference {domain | host}
    set smtp-eom-bare-lf-handling {allow | disallow | ignore}
    set smtp-max-connections <connections_int>
    set smtp-max-hop-count <hops_int>
    set smtp-msa {enable | disable}
    set smtp-msa-port <port_int>
    set smtp-mtasts-status {check-all-domain | check-external-domain | disable}
    set smtp-port <port_int>
    set smtp-service {enable | disable}
    set smtps-port <port_int>
    set smtp-smtputf8 {enable | disable}
    set smtps-tls-status {enable | disable}
    set timeout-connect <seconds_int>
    set timeout-greeting <seconds_int>
end
```

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

Variable	Description	Default
delivery-failure-conditions {dns-failure | mta-failure-permanant | mta-failure-temporary | network-failure-connection | network-failure-other}	Select which type of failed network connections that the backup relay should take over and retry. Also configure delivery-failure-handling-option {normal | relay-to-host}.	
delivery-failure-handling-option {normal | relay-to-host}	Select what to do when email delivery failstemporarily or permanently. • `normal`: Queue the email on FortiMail and use the mail queue settings. • `relay-to-host`: Use another relay (backup relay) that you want to use for failed deliveries. Also configure delivery-failure-host <host_name>.	normal
delivery-failure-host <host_name>	Enter a host to relay email when access to original mail host fails.	
delivery-failure-min-age <minutes_int>	Enter the time in minutes the undelivered email should wait in the normal queue before trying the backup relay.	30
delivery-tracking-status {enable | disable}	Enable to record the following mail delivery statuses in the history log: • Delivered • Blocked • Failed • Queued You can view queued email except IBE email in the history log from the right-click pop-up menu. For security reasons, IBE email cannot be viewed in the queue.	disable
dsn-ehlo-option {host-name | domain-name | other-name}	Specify the DSN `EHLO`/`HELO` argument to use: • `host-name`: Use the host name of the FortiMail unit. • `domain-name`: Use the local domain name of the FortiMail unit. • `other-name`: Use a customized name specified in dsn-ehlo-other-name <name_str> on page 331.	host-name
dsn-ehlo-other-name <name_str>	If dsn-ehlo-option {host-name | domain-name | other-name} is `other-name`, use this command to enter the customized name.	
dsn-email-attach-orig {enable | disable}	Enable to attach original email in delivery status notifications (DSN) or non-delivery reports (NDR).	disable
dsn-email-customization-status {enable | disable}	Enable DSN and NDR customization.	disable

Variable	Description	Default
dsn-sender-address <email_str>	Enter the sender email address in DSN email messages sent by the FortiMail unit to notify email users of delivery failure. If this string is empty, the FortiMail unit sends DSN from the default sender email address of “postmaster@example.com", where “example.com" is the domain name of the FortiMail unit.	
dsn-sender-displayname <name_str>	Enter the display name of the sender email address for DSN. If this string is empty, the FortiMail unit uses the display name “postmaster".	
dsn-status {enable | disable}	Enable to allow DSN email generation.	disable
imap-service {enable | disable}	Enable to allow IMAP service.	enable
ip-pool-direction {all | exclude-internal-to-internal}	By default, IP pools in IP policies and domain settings will be applied to all email directions, including internal to internal, internal to external, external to internal, and external to external. You can exempt IP pool usage for internal-to-internal email using the `exclude-internal-to-internal` option. **Note:** IP pools in ACL delivery rules are still applied to internal-to-internal email.	
ldap-domaincheck {enable | disable}	Enable to verify the existence of domains that have not been configured as protected domains. Also configure `ldap-domaincheck-profile <profile_str>` and `ldap-domaincheck-auto-associate {enable | disable}`. To verify the existence of unknown domains, the FortiMail unit queries an LDAP server for a user object that contains the email address. If the user object exists, the verification is successful, the action varies by configuration of `ldap-domaincheck-auto-associate {enable | disable}`.	disable
ldap-domaincheck-auto-associate {enable | disable}	If ldap-domaincheck {enable | disable} is `enable`, select whether to enable or disable automatic creation of domain associations. • `enable`: The FortiMail unit automatically adds the unknown domain as a domain associated of the protected domain selected in `ldap-domaincheck-internal-domain <domain_str>`. • `disable`: If the DNS lookup of the unknown domain name is successful, the FortiMail unit routes the email to the IP address resolved for the domain name during the DNS lookup. Because the domain is not formally defined as a protected domain, the email is considered to be outgoing, and outgoing recipient-based policies are used to scan the email. For more information, see policy recipient on page 156.	disable

Variable	Description	Default
ldap-domaincheck-internal-domain <domain_str>	If ldap-domaincheck {enable | disable} is `enable`, and ldap-domaincheck-auto-associate {enable | disable} is `enable`, enter name of the protected domain with which successfully verified domains will become associated.	
ldap-domaincheck-profile <profile_str>	If ldap-domaincheck {enable | disable} is `enable`, enter the name of the LDAP profile to use when verifying unknown domains.	
local-domain-name <local-domain_str>	Enter the name of the domain to which the FortiMail unit belongs, such as `example.com`. This option applies only if the FortiMail unit is operating in server mode.	
pop3-port <port_int>	Enter the port number on which the FortiMail unit's POP3 server will listen for POP3 connections. The default port number is 110. This option applies only if the FortiMail unit is operating in server mode.	110
pop3-service {enable | disable}	Enable to allow POP3 service.	enable
queue-dsn-timeout <days_int>	Select the maximum number of hours a delivery status notification (DSN) can remain in the default, incoming, or outgoing queues. After it reaches the maximum, the FortiMail unit moves the DSN email to the dead mail folder. If this setting is `0`, then the FortiMail unit does not retry for DSN. Valid range is 0 to 10.	5
queue-max-delivery-attempt <tries_int>	Enter the maximum number of tries to send an email in the default, incoming, or outgoing mail queues. Valid range is 0 to 144. Entering 0 means no limit. Alternatively, configure queue-timeout <hours_int>. FortiMail applies whichever occurs first.	0
queue-max-delivery-attempt-on-dsn <tries_int>	Enter the maximum number of tries to send a delivery status notification (DSN) message in the mail queue. Valid range is 0 to 144. Entering 0 means no limit. Alternatively, configure queue-timeout <hours_int>. FortiMail applies whichever occurs first.	0
queue-regular-delivery-attempt <tries_int>	Enter the number of tries for a delivery in the default, incoming, or outgoing mail queues. If delivery is not successful, then the email is moved to a slow mail queue. Valid range is from 1 to 3. **Tip:** Slow queues also try to use queue-retry <minutes_int>, but if FortiMail is busy and system resource usage is high, then slow queues have a lower priority than normal queues, so a retry in a slow queue might not occur exactly at the interval time.This allows the FortiMail unit to send valid email more quickly, instead of wasting system resources frequently retrying email that may be invalid (for example, email destined to an invalid MTA) or for an MTA that is too busy or undergoing maintenance.	3

Variable	Description	Default
	Slow queues are created automatically; you do not need to create them in config mail-queue.	
queue-retry <minutes_int>	Enter the number of minutes between delivery retries for email in the deferred and spam mail queues. Valid range is from 5 to 120. **Note:** This interval only applies to the 1st through 3rd delivery retries.On the 4th retry or later, 20 more minutes will be added for each retry. For example, if the time interval is set to 5 minutes, the 4th retry will be 25 minutes later, the 5th retry will be 45 minutes later, and the 6th retry will be 65 minutes later. **Note:** If system resource usage is very high, then retries may be slower than this interval.	15
queue-timeout <hours_int>	Enter the maximum number of hours that email can remain in the default, incoming, or outgoing mail queues. During this time, the FortiMail unit periodically retries to send the email. If retries were not successful, and expiry occurs, then the FortiMail unit sends a final delivery status notification (DSN) email to notify the sender that the email was not deliverable. Valid range is from 1 to 240. Alternatively, configure queue-max-delivery-attempt <tries_int>. FortiMail applies whichever occurs first.	72
queue-warning <hours_int>	Select the number of hours after the 1st delivery failure to deliver the 1stdelivery status notification (DSN) message, notifying the sender that the email was delayed. Valid range is from 1 to 24.	2
relay-server-name <relay_name>	Enter the name of the relay server that will deliver outgoing email. See also mailsetting relay-host-list on page 130.	
relay-server-status {enable |disable}	If enabled, the relay server will be used to deliver outgoing email. If disabled, the FortiMail built-in MTA will be used.	disable
show-accept-cert-ca {enable | disable}	Enable to show acceptable client certificate CA.	enable
smtp-auth {enable | disable}	Enable to accept the AUTH command to authenticate email users for connections using SMTP.	enable
smtp-auth-over-tls {enable | disable}	Enable to accept the AUTH command to authenticate email users for connections using SMTP over TLS.	enable
smtp-auth-smtps {enable | disable}	Enable to accept the AUTH command to authenticate email users for connections using SMTPS (SMTP with SSL).	enable
smtp-delivery-addr-pref {ipv4-ipv6 | ipv6-ipv4 | ipv4 | ipv6}	When FortiMail delivers email to a host name, it does DNS AAAA and A record lookup. Use this command to specify the IPv4/IPv6 delivery preferences:	ipv4-ipv6

Variable	Description	Default
	• `ipv4-ipv6`: Try to deliver to the IPv4 address first. If the IPv4 address is not accessible, try the IPv6 address. Because most MTAs support IPv4, this is the default setting. • `ipv6-ipv4`: Try IPv6 first, then IPv4. However, if the AAAA record does not exist, the extra AAAA DNS lookup for IPv6 addresses will potentially cause email delivery delay. • `ipv4`: Try IPv4 only. This setting is not recommended. • `ipv6`: Try IPv6 only. This setting is not recommended.	
smtp-delivery-session-preference {domain | host}	Select how to handle recipient domain names that resolve to the same MTA: • `host`: Send the emails to the server in the **same** SMTP session. • `domain`: Send the emails in **separate** sessions. **Tip:** Select this option if you use Google business email service. It does not accept multiple destination domains per SMTP transaction, resulting in repeated delivery attempts and delayed email.	domain

smtp-eom-bare-lf-handling {allow | disallow | ignore}	Normally, to signal the end of the email, the message body should end with an end-of-message (EOM):
	`<CR><LF>.<CR><LF>`
	where `<CR>` is a carriage return and `<LF>` is a line feed.
	However in SMTP servers that are not RFC-compliant, or with attackers, the email does not end with a valid EOM. Instead its EOM is not complete, such as:
	`<LF>.<CR><LF>`
	and then continues with more email and attachments, often from other senders, nested within the same message body as an implicit pipeline. Attacks that use this are called SMTP smuggling.
	Select either:
	• `allow`: Accept the message body, but clean up and replace each bare LF or CR between email with a valid EOM, which splits the message body and normalizes the EOMs for downstream email servers and clients. Same behavior as FortiMail 7.4 and older.
	Caution: If a nested email is from a different sender, they may not be authenticated. To reduce this risk, you can use other features. For example, you could disable smtp-diff-identity {enable | disable} and enable dkim-checking {enable | disable}.
	• `ignore`: Accept the message body, and keep the bare LF or CR between email as-is so that the message body is still together for downstream mail servers and clients.
	• `disallow`: Reject the message body if it contains a bare LF or CR. This option is most secure, but is not compatible with non-standard email servers. If you want to disable explicit pipelining too, configure session-allow-pipelining {yes | no}.
		allow

Variable	Description	Default
	Note: For `allow` and `ignore`, FortiMail still requires that the last EOM is valid. It waits up to 3 minutes for it. If it does not occur, then the action may be different: • `allow`: Rejects the last email only, with a log message that explains a bad pipeline. • `ignore`: Rejects all email in the nested message body, with log messages that explain a bare LF or bare CR, similar to `disallow`.	
smtp-max-connections <connections_int>	Enter the maximum number of concurrent SMTP connections that FortiMail can accept from the SMTP clients.	Platform dependent
smtp-max-hop-count <hops_int>	Enter the maximum number of hops that FortiMail can accept from the SMTP connections. Valid range is 1 to 200.	30
smtp-msa {enable | disable}	Enable to allow your email clients to use SMTP for message submission on a separate TCP port number from deliveries or mail relay by MTAs. For details on message submission by email clients as distinct from SMTP used by MTAs, see RFC 2476.	disable
smtp-msa-port <port_int>	Enter the TCP port number on which the FortiMail unit listens for email clients to submit email for delivery.	587
smtp-mtasts-status {check-all-domain | check-external-domain | disable}	Enable MTA Strict Transport Security (MTA-STS) domain checking: • `check-all-domain`: FortiMail checks recipient domain MTA-STS records (including TLS version, format, and MTA-STS policy) for outgoing email to both internal and external domains. • `check-external-domain`: FortiMail MTA-STS checking only when delivering outgoing emails to external domains. • `disable`: Disable MTA-STS domain checking.	disable
smtp-port <port_int>	Enter the port number on which the FortiMail unit's SMTP server will listen for SMTP connections.	25
smtp-service {enable | disable}	Enable to allow SMTP service.	disable
smtp-smtputf8 {enable | disable}	Enable for UTF-8 support in SMTP session commands and message headers. This allows non-ASCII characters in email addresses and international domain names (IDN) in `EHLO` hostnames and the domain parts of email addresses. For example, non-ASCII recipient email addresses must be followed by the `SMTPUTF8` keyword: `RCPT TO: <pelé@example.com> SMTPUTF8` Disable if SMTP clients are not compatible with SMTPUTF8. For details, see RFC 6530, RFC 6531, RFC 6532, and RFC 6533.	disable
smtps-port <port_int>	Enter the port number on which the FortiMail unit's built-in MTA listens for secure SMTP connections.	465
smtps-tls-status {enable | disable}	Enable to allow SSL- and TLS-secured connections from SMTP clients that request SSL/TLS.	disable

Variable	Description	Default
	When disabled, SMTP connections with the FortiMail unit's built-in MTA must occur as clear text, unencrypted.	
timeout-connect <seconds_int>	Enter the maximum amount of time to wait, after the FortiMail unit initiates it, for the receiving SMTP server to establish the network connection. Valid range is 10 to 120. **Note:** This timeout applies to all SMTP connections, regardless of whether it is the first connection to that SMTP server or not.	30
timeout-greeting <seconds_int>	Enter the maximum amount of time to wait for an SMTP server to send SMTP reply code 220 to the FortiMail unit. Valid range is 10 to 360. **Note:** RFC 2821 recommends a timeout value of 5 minutes (300 seconds). For performance reasons, you may prefer to have a smaller timeout value, which reduces the amount of time spent waiting for sluggish SMTP servers. However, if this causes your FortiMail unit to be unable to successfully initiate an SMTP session with some SMTP servers, consider increasing the timeout.	30

Related topics

system dns

system route

mailsetting relay-host-list

system encryption ibe

system password-policy

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

Syntax

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

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

Related topics

system link-monitor

system port-forwarding

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

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

Before you do the mapping, make sure both ports are open.

Syntax

```
config system port-forwarding
   edit <route_int>
      set destination <destination_ipv4mask>
      set gateway <gateway_ipv4>
end
```

Variable	Description	Default
<number>	Enter the index number of the entry.	
dst-host <calss_ip>	Enter the IP address of the host where the packets will be forwarded.	0.0.0.0
dst-port <port_number>	Enter the port number of the destination host.	0
host <class_ip>	Enter the IP address of the FortiMail interface where the packets are received.	0.0.0.0
port <port_number>	Enter the port number on the FortiMail interface where the packets are received.	0
protocol {tcp | udp | both}	Specify the protocol of the traffic.	tcp

system route

Use this command to configure static routes.

Syntax

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

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

Variable	Description	Default
gateway <gateway_ipv4>	Enter the IP address of the gateway router.	0.0.0.0
interface <interface_name>	Enter the interface name that you want to add the static route to.	

Related topics

system link-monitor

system saml

Use this command to configure FortiMail to act as a SAML SSO service provider (SP).

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

- FortiMail, which is the service provider (SP)
- FortiAuthenticator or other remote authentication server, which is the identity provider (IdP). See profile sso on page 260.

When you enable SSO, FortiMail automatically generates its SP metadata XML, entity ID, and ACS URL. (To download them, use the GUI.)

Syntax

```
config system saml
   set status {enable | disable}
   set dynamic-ip-status {enable | disable
   set dynamic-ip {<client_ipv4/mask>,...}
end
```

Variable	Description	Default
status {enable | disable}	Enable or disable the feature.	disable
dynamic-ip {<client_ipv4/mask>,...}	Enter the IdP's client IP addresses or subnet in CIDR or dotted decimal format. Separate multiple IP addresses or subnets with a comma. Spaces are not allowed. If no IP range is specified, then any IP address is allowed. **Tip:** For better security, only allow IdP communications from known IP addresses.	
dynamic-ip-status {enable | disable	Enable if the IdP uses dynamic client IP addresses, even within the same SAML session. (This can be useful, for example, if the IdP is deployed behind a load balancer.) Also configure dynamic-ip {<client_ipv4/mask>,...}.	disable

Related topics

profile sso
system appearance

system scheduled-backup

Use this command to configure system configuration backup. You can choose to back up the configurations locally or remotely. You can also specify the backup schedules.

Syntax

```
config system scheduled-backup
   set destination {local | remote} on page 341
   set max-backup-num <integer> on page 341
   set remote-directory <string> on page 341
   set remote-host <string> on page 341
   set remote-password <string> on page 341
   set remote-protocol {ftp | sftp} on page 341
   set remote-username <string> on page 341
   set schedule {daily | none | weekdays} on page 341
   set schedule-hour <integer> on page 342
   set schedule-weekdays {monday ... sunday} on page 342
end
```

Variable	Description	Default
destination {local | remote}	Select whether to back up on the local machine and/or remotely on a FTP/SFTP server.	`local`
max-backup-num <integer>	Set the maximum number of backup to keep. When the number is reached, the oldest version will be overwritten. Valid range is 1 to 52.	`10`
remote-directory <string>	Specify the storage directory on the remote server.	
remote-host <string>	Specify the host name or IP address of the remote server.	
remote-password <string>	Specify the password to log on to the remote server.	
remote-protocol {ftp | sftp}	Specify either FTP or SFTP.	`sftp`
remote-username <string>	Specify the user name to log on to the remote server.	
schedule {daily | none | weekdays}	You can choose to back up daily or on specify day/days (from Monday to Sunday), or not back up at all (none).	

Variable	Description	Default
schedule-hour <integer>	Specify the time (from 1 to 24) to perform the backup.	23
schedule-weekdays {monday ... sunday}	If you choose the weekday backup schedule, specify the day/days (from Monday to Sunday).	sunday

system security crypto

Use this command to modify protocol-specific cryptography settings for HTTPS and SMTPS (SSL/TLS) secure connections. (Other protocols use settings in system global.)

Syntax

```
config system security crypto
   edit http
      set custom-ciphers <ciphers_str>
      set dh-params {1024 | 2048 | 3072 | 4096}
      set ssl-versions {tls1_0 tls1_1 tls1_2 tls1_3}
      set status {enable | disable}
      set strong-crypto {enable | disable}
   edit mail
      set custom-ciphers <ciphers_str>
      set dh-params {1024 | 2048 | 3072 | 4096}
      set ssl-versions {tls1_0 tls1_1 tls1_2 tls1_3}
      set status {enable | disable}
      set strong-crypto {enable | disable}
end
```

Variable	Description	Default

custom-ciphers <ciphers_str>	Select which ciphers FortiMail will accept in HTTPS and SMTPS secure connections from clients.
	To display a list of cipher options and the current selection, type:
	`set custom-ciphers ?`
	In the *Available ciphers* section is the list of ciphers that this FortiMail firmware version supports. In the *Selected ciphers* section is the list ciphers that you have selected to allow.
	To add cipher suites to the list, type + before the name of each cipher, and separate multiple names with spaces, such as:
	`+RC4-SHA +CAMELLIA256-SHA`
	To delete cipher suites from the list, type - before the name of each cipher, and separate multiple names with spaces, such as:
	`-RC4-SHA -CAMELLIA256-SHA`	

Variable	Description	Default
dh-params {1024 | 2048 | 3072 | 4096}	Enter the minimum size of the Diffie-Hellman prime number for secure connections such as SSH, SMTPS, and HTTPS. Larger bit sizes are slower to generate, but generally more secure. Alternatively, you can set the Diffie-Hellman bit size globally. See system global on page 311.	2048
ssl-versions {tls1_0 tls1_1 tls1_2 tls1_3}	Select which SSL/TLS version(s) FortiMail will accept in secure connections: • from clients (HTTPS web browsers and SMTPS mail clients) • to servers (protected mail servers and Syslog with TCP over TLS) Separate multiple versions with a space. Alternatively, you can select SSL/TLS versions globally. See system global on page 311. **Note:** Some old versions of web browsers, email clients (for example, Microsoft Outlook 2007 and older), MTAs only support TLS 1.0. Therefore they cannot connect to FortiMail if you enable strong-crypto {enable | disable} and/or disable TLS 1.0.	tls1_1 tls1_2 tls1_3
status {enable | disable}	Enable to override the global settings, and apply protocol-specific cryptography settings. Disable to use system-wide settings in system global on page 311.	disable
strong-crypto {enable | disable}	Enable to use strong encryption and only allow strong ciphers (AES-128 or better) and digest (SHA-256 or better) for HTTPS and SSH access. Old SSL/TLS versions with known vulnerabilities such as SSL 3.0 are also disabled, so this setting may partially override ssl-versions {tls1_0 tls1_1 tls1_2 tls1_3}. For additional security, you can also configure custom-ciphers <ciphers_str>. Alternatively, you can enforce strong encryption globally. See system global on page 311. **Note:** Old mail clients and old browser versions such as Microsoft Internet Explorer 6.0 do not support strong encryption.	enable

Related topics

profile encryption

system global

system security authserver

Use this command to modify the tracking functions used to prevent password guessing attempts. The sender IP addresses in the exempt list will bypass the security checking.

Syntax

```
config system security authserver
      config exempt-list
         edit auth_exempt_id
            set sender-ip-mask
         end
      set access-group {cli mail web}
      set block-period <minutes>
      set status (disable | enable | monitor-only)
end
```

Variable	Description	Default
auth_exempt_id	Enter the ID for the list.	
sender-ip-mask	Enter the sender's IP address.	
access-group {cli mail web}	Enter the groups of access tracked by authserver.	cli mail web
block-period <minutes>	Enter the block period in minutes.	10
status (disable | enable | monitor-only)	Enable or disable this list.	enable

system snmp community

Use this command to configure simple network management protocol (SNMP) v1/2 settings.

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

Syntax

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

```
end
```

Related topics

system snmp sysinfo
system snmp threshold

system snmp sysinfo

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

Syntax

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

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

Related topics

system snmp community
system snmp threshold

system snmp threshold

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

Syntax

```
config system snmp threshold
   set {cpu | deferred-queue | logdisk | maildisk | mem | spam | virus} <trigger_int> <threshold_
        int> <sample_period_int> <sample_frequency_int>
end
```

Variable	Description	Default
{cpu | deferred-queue | logdisk | maildisk | mem | spam | virus} <trigger_int> <threshold_int> <sample_period_int> <sample_frequency_int>	Specify the trap event, such as cpu or spam, then specify the following threshold values: `trigger_int`: You can enter either the percent of the resource in use or the number of times the trigger level must be reached before it is triggered. For example, using the default value, if the mailbox disk is 90% or more full, it will trigger. `threshold_int`: Sets the number of triggers that will result in an SNMP trap. For example, if the CPU level exceeds the set trigger percentage once before returning to a lower level, and the threshold is set to more than one an SNMP trap will not be generated until that minimum number of triggers occurs during the sample period. `sample_period_int`: Sets the time period in seconds during which the FortiMail unit SNMP agent counts the number of triggers that occurred. This value should not be less than the Sample Frequency value. `sample_frequency_int`: Sets the interval in seconds between measurements of the trap condition. You will not receive traps faster than this rate, depending on the selected sample period. This value should be less than the Sample Period value.	cpu: 80 3 600 30 mem: 80 3 600 30 logdisk: 90 1 7200 3600 maildisk: 90 1 7200 3600 virus: 10 600 spam: 60 600

Related topics

system snmp community
system snmp sysinfo

system snmp user

Use this command to configure SNMP v3 user settings.

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

Syntax

```
config system snmp user
   edit <user_name>
      set query-status {enable | disable}
      set query-port <port_number>
      set security-level {authnopriv | authpriv | noauthnopriv}
      set auth-proto {sha1 | md5}
      set aut-pwd <password>
      set status {enable | disable}
      set trap-status {enable | disable}
      set trapevent {cpu | deferred-queue | ha | ip-change | logdisk | mem | raid | remote-
            storage | spam | system | virus}
      set trapport-local <port_number>
      set trapport-remote <port_number>
   config host
      edit <host_no>
         set ip <class_ip>
   end
end
```

Variable	Description	Default
<user_name>	Enter a name to identify the SNMP user on FortiMail.	
query-status {enable | disable}	Enable to allow SNMP v3 query from the SNMP managers. Also configure the query port as described below.	disable
query-port <port_number>	Specify the port number used to listen to queries from the SNMP manager.	161
security-level {authnopriv | authpriv | noauthnopriv}	Choose one of the three security levels for the communication between FortiMail and the SNMP manager. • `noauthnotpriv` (no authentication, no privacy): This option is similar to SNMP v1 and v2. • `authnopriv` (authentication, no privacy): This option enables authentication only. The SNMP manager needs to supply a password that matches the password you specify on FortiMail. You must also specify the authentication protocol (either SHA1 or MD5). • `authpriv` (authentication, privacy): This option enables both authentication and encryption. You must specify the protocols and passwords. Both the protocols and passwords on the SNMP manager and FortiMail must match.	
auth-proto {sha1 | md5}	Specify the authentication protocol if you choose authentication for the security level. Otherwise, this option is not displayed.	

Variable	Description	Default
aut-pwd <password>	Specify the authentication password if you choose authentication for the security level. Otherwise, this option is not displayed.	
status {enable | disable}	Enable or disable the SNMP v3 user on FortiMail.	disable
trap-status {enable | disable}	Enable to activate traps on FortiMail.	disable
trapevent {cpu | deferred-queue | ha | ip-change | logdisk | mem | raid | remote-storage | spam | system | virus}	Enter one or more of the following events that will generate a trap when the event occurs or when its threshold is reached: • `cpu`: CPU usage threshold • `deferred-queue`: Deferred queue threshold • `ha`: High availability (HA) event • `ip-change`: Interface IP address change • `logdisk`: Log disk space low threshold • `maildisk`: Mail disk space low threshold • `mem`: Memory low threshold • `raid`: RAID event • `remote-storage`: NAS storage related events • `spam`: Spam threshold • `system`: System events, such as a change in the state of hardware, power failure and so on. • `virus`: Virus threshold **Note**: Since FortiMail checks its status in a scheduled interval, not all the events will trigger traps. For example, FortiMail checks its hardware status every 60 seconds. This means that if the power is off for a few seconds but is back on before the next status check, no system event trap will be sent. To set SNMP trap thresholds for the event types that use them, see system snmp threshold on page 346. Events apply only when traps are enabled in.	cpu deferred-queue ha logdisk maildisk mem raid remote-storage system
trapport-local <port_number>	Enter the local port number for sending traps.	162
trapport-remote <port_number>	Enter the remote port number that listens to SNMP traps on the SNMP manager.	162
<host_no>	Enter an index number for the SNMP manager.	
ip <class_ip>	Enter the IP address of the SNMP manager.	

Related topics

system snmp community
system snmp sysinfo

system threat-feed

Use this command to configure threat feeds.

Threat feeds are plain text files that contain a list of security threats. Threat feeds can be hosted on FortiClient EMS, third party servers, or your own HTTP/HTTPS web server. In this way, FortiMail units can utilize security information from many vendors, security communities, and specialist teams in your own organization. Once FortiMail is connected to threat feeds, you can select them when you configure security features such as antivirus file signatures and antispam IP reputation and URL filters.

FortiMail periodically synchronizes with threat feeds and automatically imports changes.

If the threat feed's web server becomes unreachable and there is a connection status error, then the FortiMail continues to use its existing local cache of the threat feed, regardless of reboot. To get threat feed updates, you must re-establish network connectivity.

Syntax

```
config system threat-feed
   edit <profile_name>
      [set comment<comment_str>]
      set status {enable | disable}
      set type {ip-address | malware-hash | url-category}
      set resource-url <feed_url>
      set server-identity-check {basic | full | none}
      set username <user_str>
      set password <password_str>
      [set update-method {pull}]
      set update-interval <minutes_int>
   next
end
```

Variable	Description	Default
<profile_name>	Enter the name of the profile.	
comment<comment_str>	Optional description of the local category.	
password <password_str>	If the server requires authentication, enter the password that FortiMail will use to connect.	
resource-url <feed_url>	Enter the URI of the threat feed. FortiMail also supports OASIS STIX/TAXII format. To use the TAXII protocol, use the `stix://` prefix instead of `https://`.	
server-identity-check {basic | full | none}	Select the level of server certificate validation strictness, either: • none — No certificate validation. • basic — Validate the server certificate. It must not be revoked or	none

Variable	Description	Default
	expired, and must be signed by a trusted CA. See also system certificate ca on page 284. • `full` — In addition to validation requirements in `basic`, the domain name in resource-url <feed_url> must match the common name (CN) field in the server certificate.  To harden security, select `full`.	
status {enable | disable}	Enable or disable the threat feed.	enable
type {ip-address | malware-hash | url-category}	Select the type of threat feed, either: • `ip-address` — IPv4 or IPv6 addresses. • `malware-hash` — MD5, SHA1, or SHA256 file checksums. • `url-category` — URIs such as `https://example.com:4443/url/*` For details on the types and their required file format, see the FortiMail Administration Guide.	ip-address
update-interval <minutes_int>	Enter the frequency in minutes of synchronization with the threat feed. Default value is 30 minutes. Valid range is from 1 to 43200 minutes (30 days).	30
update-method {pull}	Currently, only the pull method of threat feed synchronization is supported.	pull
username <user_str>	If the server requires authentication, enter the username that FortiMail will use to connect.	

Related topics

file signature
profile antispam
system webfilter customized-category

system time manual

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

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

This command applies only if NTP is disabled. Alternatively, you can configure the FortiMail unit to synchronize its system time with an NTP server. For details, see system time ntp on page 351.

Syntax

```
config system time manual
   set daylight-saving-time {disable |  enable}
   set zone {0 | .. | 90}
end
```

Variable	Description	Default
daylight-saving-time {disable | enable}	Enable to automatically adjust the system time for daylight savings time (DST).	enable
zone {0 | .. | 90}	Enter the number that indicates the time zone in which the FortiMail unit is located. Valid range is 0-90.	12

Related topics

system time ntp

system time ntp

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

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

Alternatively, you can manually configure the system time of the FortiMail unit. For details, see system time manual on page 350.

Syntax

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

Variable	Description	Default
ntpserver {<address_ipv4> | <fqdn_str>}	Enter either the IP address or fully qualified domain name (FQDN) of an NTP server. You can add a maximum of 10 NTP servers. The FortiMail unit uses the first NTP server based on the selection mechanism of the NTP protocol. To locate a public NTP server, visit http://www.ntp.org/.	pool.ntp.org

Variable	Description	Default
ntpsync {enable | disable}	Enable to synchronize the FortiMail unit with an NTP server, instead of manually configuring the system time.	enable
syncinterval <interval_int>	Enter the interval in minutes between synchronizations of the system time with the NTP server. The valid range is from 1 to 1440 minutes.	60

Related topics

system time manual

system wccp settings

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

Syntax

```
config system wccp settings
   set authentication
   set id
   set local-ip
   set password
   set remote-ip
   set status
end
```

Variable	Description	Default
authentication	Enable or disable authentication.	
id	Enter the ID of the tunnel.	
local-ip	Enter the ip address of the local interface.	
password	Enter the authentication password.	
remote-ip	Enter the ip address of the remote server.	
status	Enable or disable WCCP mode.	
file_name <file_str>	Enter the name of the language resource file, such as `'custom_french1'`.	

system web-service

Use this command to configure the rate limit for REST APIs, including the maximum concurrent REST API requests (overall and for individual IP addresses), and how fast the system should perform, in terms of how many requests and responses are processed per second. It also configures connections for FortiMail webmail and per-user quarantines.

Valid value ranges for certain commands vary by FortiMail model. See FortiMail Maximum Values.

Syntax

```
config system web-service
   set https-redirect-status {enable | disable}
   set https-redirect-host <fortimail_fqdn>
   set max-active-session-admin <limit_int>
   set max-active-session-restful <limit_int>
   set max-concurrent-request-admin <limit_int>
   set max-concurrent-request-all <limit_int>
   set max-concurrent-request-ms365 <limit_int>
   set max-concurrent-request-per-ip <limit_int
   set max-concurrent-request-restful <limit_int>
   set max-concurrent-request-webmail <limit_int>
   set max-request-rate-admin <limit_int>
   set max-request-rate-ms365 <limit_int>
   set max-request-rate-restful <limit_int>
   set max-request-rate-webmail <limit_int>
   set rest-api-status {enable | disable}
   set webmail-session-ttl <seconds_int>
   config exempt-list
      edit <list_index>
         set <client_ipv4mask>
      next
   end
end
```

Variable	Description	Default
<list_index>	Enter a number to identify the entry.	
<client_ipv4mask>	Enter an IP address and netmask that you want to exempt from concurrent request rate limits.	
https-redirect-status {enable | disable}	Enable to redirect insecure HTTP requests to secure access using HTTPS. This setting affects all FortiMail URLs: REST APIs, administrator GUI, FortiMail webmail, and per-user quarantines.	enable

Variable	Description	Default
	Note: For this setting to take effect, you must also enable both HTTP and HTTPS access protocols on the network interface (s) that receive these connections. FortiMail cannot redirect HTTP if it is not listening for it. See allowaccess {ping http https snmp ssh telnet} on page 324.	
https-redirect-host <fortimail_fqdn>	Enter the fully qualified domain name (FQDN) to use in HTTPS redirects.	
max-active-session-admin <limit_int>	Enter the maximum number of active administrator sessions.	200
max-active-session-restful <limit_int>	Enter the maximum number of active RESTful sessions.	10
max-concurrent-request-admin <limit_int>	Enter the maximum number of concurrent admin portal requests.	50
max-concurrent-request-all <limit_int>	Enter the maximum number of concurrent HTTP requests from all clients.	0
max-concurrent-request-ms365 <limit_int>	Enter the maximum number of concurrent Microsoft Office 365 requests permitted.	100
max-concurrent-request-per-ip <limit_int	Enter the maximum number of concurrent HTTP requests for a single IP address.	0
max-concurrent-request-restful <limit_int>	Enter the maximum number of concurrent RESTful requests.	20
max-concurrent-request-webmail <limit_int>	Enter the maximum number of concurrent webmail portal requests.	200
max-request-rate-admin <limit_int>	Enter the maximum request rate (per second) for administrators.	0
max-request-rate-ms365 <limit_int>	Enter the maximum request rate (per second) for Microsoft Office 365.	100
max-request-rate-restful <limit_int>	Enter the maximum request rate (per second) to the REST API.	50
max-request-rate-webmail <limit_int>	Enter the maximum request rate (per second) for webmail.	0
rest-api-status {enable | disable}	Enable or disable REST API access. **Note**: For this setting to take effect, you must also enable HTTPS access protocols on the network interface(s) that receive these connections. FortiMail cannot respond to an API requestif it is not listening for it. See allowaccess {ping http https snmp ssh telnet} on page 324.	disable
webmail-session-ttl <seconds_int>	Enter the amount of time, in seconds, that an inactive FortiMail webmail session is still valid. The maximum value is 600 seconds (10 minutes). Enter `0` to effectively disable the session keepalive.	60

Variable	Description	Default
	While a webmail user is logged in, their browser periodically sends a request to FortiMail. This GUI heartbeat keeps the session alive — even if the user is idle (they do not open any email,etc.). Heartbeats are not sent if the • user closes the browser tab or window • network connection is interrupted — even temporarily FortiMail waits for the heartbeat to reconnect. If it does not (the session time to live (TTL) elapses), then the session expires and the user is automatically logged out. Otherwise an idle session can continue until the idle timeout occurs (see idle-timeout {enable | disable}). **Tip:** If your network connection is reliable, you can use a smaller session TTL for better security and performance. **Note:** Before the session TTL elapses, users may still need to log in again if they: • log out • clear cookies • open a new incognito/private browser tab or window	

Related topics

system interface

system webfilter customized-category

Use this command to configure your own custom URL rating categories.

When you configure a custom category via CLI, its `group` and `id` are assigned automatically. To view the `group` and `id` of categories that you have configured, enter:

```
config system webfilter customized-category
   show
```

Some IDs are reserved for use by predefined categories and threat feeds. See the FortiMail Administration Guide.

For exemptions, you can use the predefined category `local-exempt`.

Syntax

```
config system webfilter customized-category
   edit <category_name>
      [set description <description_str>
      [set threat-feed <feed_name>]
   next
end
```

Variable	Description	Default
<category_name>	Enter a name for the custom category.	
description <description_str>	Enter a description or comment.	
threat-feed <feed_name>	If you want the groupto be `remote` (that is, the custom category of URLs is defined on a remote web server), then enter the name of the threat feed. Else do not configure this setting, and then `group` will automatically be `local`.	

Related topics

antispam settings

profile url-filter

system webfilter local-rating

system threat-feed

system webfilter local-rating

Use these commands to configure URL rating overrides.

You can override and assign a different rating category to URLs. This can be useful if, for example:

- A shared web server hosts multiple different apps, and one of the URLs must be filtered differently.
- A FortiGuard URL rating is temporarily incorrect and you want to create an exemption.

Syntax

```
config system webfilter local-rating
   edit <override_index>
      [set description <description_str>
      set status {enable | disable}
      set pattern-type {regexp | wildcard}
      set url-pattern <url_pattern>
```

```
    set category <category_name>
  next
end
```

Variable	Description	Default
<override_index>	Enter the number of the override.	
category <category_name>	Select which category to assign to the URLs that match url-pattern <url_pattern>, either: • a predefined category from FortiGuard, such as `spam-urls` • a predefined category from the firmware, such as `local` or `local-exempt` • a custom category (see system webfilter customized-category on page 355) To view the list of categories, enter: `set category ?`	local
description <description_str>	Enter a comment or description.	
pattern-type {regexp | wildcard}	Select the type of url-pattern <url_pattern>, either: • `wildcard` — Simple wildcards (`?` or `*`) if you need to match multiple characters. • `regexp` — Flexible and full-featured pattern matching. **Tip:** To test that a regular expression matches as expected (and does not accidentally match other text), you can click the *Validate* in the GUI. For examples and information on wildcard and regular expression syntax, see the FortiMail Administration Guide.	wildcard
status {enable | disable}	Enable or disable the override.	enable
url-pattern <url_pattern>	Enter a pattern that matches only the URLs that you want to override. Syntax varies by pattern-type {regexp | wildcard}.	*

Related topics

antispam settings

system webfilter customized-category

system webmail-language

Use this command to create or rename a webmail language.

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

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

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

Syntax

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

Variable	Description	Default
en_name <language-name-en_str>	Enter the name of the language in English, such as `'French'`. Available languages vary by whether or not you have installed additional language resource files.	
name <language-name_str>	Enter the name of the language, such as `'Français'`.	
file_name <file_str>	Enter the name of the language resource file, such as `'custom_french1'`.	

Related topics

config user mail

user alias

Use this command to configure email address aliases.

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

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

Resolving aliases to real email addresses enables the FortiMail unit to send a single spam report and maintain a single quarantine mailbox at each user's primary email account, rather than sending separate spam reports and maintaining separate quarantine mailboxes for each alias email address. For FortiMail units operating in server mode, this means that users need only log in to their primary account in order to manage their spam quarantine, rather than logging in to each alias account individually.

Alternatively, you can configure an LDAP profile in which the alias query is enabled. For details, see profile ldap on page 221.

Syntax

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

Variable	Description	Default
name <email-alias_str>	Enter the email address that is the alias, such as `alias1@example.com`.	
member '<recipient_str>'	Enter a recipient email addresses to which the alias will translate or expand. The email addresses may be members of either mail domains that are protected by the FortiMail unit, members of mail domains that are unprotected, or a mixture of the two. Separate each email address with a comma, and enclose the list in single quotes (').	

Related topics

user map

user pki

user map

Use this command to configure email address mappings.

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

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

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

Mappings cannot translate one email address into many.

Mappings cannot translate an email address into one that belongs to an unprotected domain (this restriction applies to locally defined address mappings only. This is not enforced for mappings defined on an LDAP server).

Mappings are applied bidirectionally, when an email is outgoing as well as when it is incoming to the protected domain.

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

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

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

Match evaluation and rewrite behavior for email address mappings

Order of evaluation	Match condition	If yes...	Rewrite to...
1	Does `RCPT TO:` match an **external** email address?	Replace `RCPT TO:`.	Internal email address

2	Does `MAIL FROM:` match an **internal** email address?	For each of the following, if it matches an internal email address, replace it:
		`MAIL FROM:`
		`RCPT TO:`
		`From:`
		`To:`
		`Return-Path:`
		`Cc:`
		`Reply-To:`
		`Return-Receipt-To:`
		`Resent-From:`
		`Resent-Sender:`
		`Delivery-Receipt-To:`
		`Disposition-Notification-To:`
			External email address

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

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

Alternatively, you can configure an LDAP profile to query for email address mappings. For details, see profile ldap on page 221.

Syntax

```
config user map
   edit encryption-profile <profile_name>
      set external-name <pattern_str>
end
```

Variable	Description	Default
internal-name <pattern_str>	Enter either an email address, such as `user1@example.com`, or an email address pattern, such as `*@example.com`, that exists in a protected domain. This email address will be rewritten into `external-name <pattern_str>` according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings on page 360. **Note**: If you enter a pattern with a wild card (`*` or `?`): You must enter a pattern using the same wild card in `external-name <pattern_str>`. The wild card indicates that the mapping could match many email addresses, but also indicates, during the rewrite, which substring of the original email address will be substituted into the position of the wild card in the external address. If there is no wild card in the other half of the mapping, or the wild card is not the same (that is, * mapped to ? or vice versa), this substitution will fail. `external-name <pattern_str>` must not be within the same protected domain. This could cause situations where an email address is rewritten twice, by matching both the sender and recipient rewrite conditions, and the result is therefore the same as the original email address and possibly not deliverable.	
external-name <pattern_str>	Enter either an email address, such as `user2@example.com`, or an email address pattern, such as `*@example.net`, that exists in a protected domain. This email address will be rewritten into encryption-profile <profile_name> according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings on page 360. **Note:** If you enter a pattern with a wild card (`*` or `?`): You must enter a pattern using the same wild card in encryption-profile <profile_name>. The wild card indicates that the mapping could match many email addresses, but also indicates, during the rewrite, which substring of the original email address will be substituted into the position of the wild card in the internal address. If there is no wild card in the other half of the mapping, or the wild card is not the same (that is, * mapped to ? or vice versa), this substitution will fail.	

Variable	Description	Default
	encryption-profile <profile_name> must not be within the same protected domain. This could cause situations where an email address is rewritten twice, by matching both the sender and recipient rewrite conditions, and the result is therefore the same as the original email address and possibly not deliverable.	

Related topics

system wccp settings

user pki

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

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

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

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

If the client certificate is **not** valid, depending on whether you have configured the FortiMail unit to require valid certificates (see certificate-required {yes | no} for FortiMail webmail users, and pki-certificate-req {yes | no} for FortiMail administrators), authentication will either fail absolutely, or fail over to a user name and password mode of authentication.

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

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

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

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

- Import the CA certificate into the FortiMail unit. For information on uploading a CA certificate, see the FortiMail Administration Guide.
- For PKI users that are FortiMail administrators, select the PKI authentication type and select a PKI user to which the administrator account corresponds. For more information, see system admin on page 275.
- For PKI users that are email users, enable PKI user authentication for the recipient-based policies which match those email users.

This command takes effect only if PKI authentication is enabled by pki-mode {enable | disable}.

Syntax

```
config user pki
   edit name <user_name>
      set ca <certificate_str>
      set domain <protected-domain_name>
      set ldap-field {cn | subjectalternative}
      set ldap-profile <profile_name>
      set ldap-query {enable | disable}
      set ocsp-ca <remote-certificate_str>
      set ocsp-check {enable | disable}
      set ocsp-unavailable-action {revoke |  ignore}
      set ocsp-URL <url_str>
      set subject <subject_str>
end
```

Variable	Description	Default
name <user_name>	Enter the name of the PKI user.	
ca <certificate_str>	Enter the name of the CA certificate used when verifying the CA's signature of the client certificate. For information on uploading a CA certificate, see the FortiMail Administration Guide.For more information, see "CA certificate". If you configure an empty string for this variable, then you must configure `subject <subject_str>`.	
domain <protected-domain_name>	Enter the name of the protected domain to which the PKI user is assigned, or enter `system` if the PKI user is a FortiMail administrator and belongs to all domains configured on the FortiMail unit. For more information on protected domains, see dlp scan-rules on page 84.	
ldap-field {cn | subjectalternative}	Enter the name of the field in the client certificate (either CN or Subject Alternative) which contains the email address of the PKI user, either `subjectalternative` (if the field is a Subject Alternative) or `cn` (if the field is a common name).	subject

Variable	Description	Default
	This email address will be compared with the value of the email address attribute for each user object queried from the LDAP directory to determine if the PKI user exists in the LDAP directory. This variable is used only if `ldap-query` is `enable`.	
ldap-profile <profile_name>	Enter the LDAP profile to use when querying the LDAP server for the PKI user's existence. For more information on LDAP profiles, see profile ldap on page 221. This variable is used only if `ldap-query` is `enable`.	
ldap-query {enable | disable}	Enable to query an LDAP directory, such as Microsoft Active Directory, to determine the existence of the PKI user who is attempting to authenticate. Also configure ldap-profile <profile_name> and ldap-field {cn | subjectalternative}.	disable
ocsp-ca <remote-certificate_str>	Enter the name of the remote certificate that is used to verify the identity of the OCSP server. For information on uploading a remote (OCSP) certificate, see the FortiMail Administration Guide. For more information, see "Remote". This option applies only if `oscpverify` is `enable`.	
ocsp-check {enable | disable}	Enable to use an Online Certificate Status Protocol (OCSP) server to query whether the client certificate has been revoked. Also configure ocsp-URL <url_str>, ocsp-ca <remote-certificate_str>, and ocsp-unavailable-action {revoke | ignore}.	disable
ocsp-unavailable-action {revoke | ignore}	Enter the action to take if the OCSP server is unavailable. If set to ignore, the FortiMail unit allows the user to authenticate. If set to revoke, the FortiMail unit behaves as if the certificate is currently revoked, and authentication fails. This option applies only if ocsp-check {enable | disable} is `enable`.	ignore
ocsp-URL <url_str>	Enter the URL of the OCSP server. This option applies only if ocsp-check {enable | disable} is `enable`.	
subject <subject_str>	Enter the value which must match the "subject" field of the client certificate. If empty, matching values are not considered when validating the client certificate presented by the PKI user's web browser. The FortiMail unit will use a CA certificate to authenticate a PKI user only if the subject string you enter here also appears in the CA certificate subject. If no subject is entered here, the subject not considered when the FortiMail unit selects the certificate to use. To disable Subject verification, enter an empty string surrounded by single quotes (''). If you configure an empty string for this variable, you must configure ca <certificate_str>.	

Related topics

system wccp settings

user map

execute

`execute` commands perform immediate operations on the FortiMail unit.

This chapter describes the following `execute` commands:

backup

Use this command to back up the configuration file to an FTP, TFTP, SCP server or your computer.

This command does **not** produce a complete backup. For information on how to back up other configuration files such as Bayesian databases, see the FortiMail Administration Guide.

Syntax

```
execute backup {config | full-config | ibe-data | mail-queue | user-config} {ftp | local | scp |
    tftp}
```

Variable	Description	Default
{config | full-config | ibe-data | mail-queue | user-config}	Type either: • `config`: Back up configuration changes only. The default settings will not be backed up. • `full-config`: Back up the entire configuration file (no default settings either), including the IBE data and user config. • `ibe-data`: Back up the IBE data. • `mail-queue`: Back up the mail queues. • `user-config`: Back up the user-specific configurations, such as user preferences, personal blocklists/safelists, and secondary addresses. Before backing up, you should update the user configuration file. To update the configurations, see user-config on page 414.	
{ftp | local | scp | tftp}	Specify the backup location and enter the file name and credentials if required.	

Example

This example uploads a password-encrypted partial configuration backup to a TFTP server.

```
execute backup full-config tftp fortimail_backup.cfg 172.16.1. 1 P@ssword1
No user configuration available!
Do you want to continue? (y/n)y
No IBE data available!
Do you want to continue? (y/n)y
System time: Tue Sep 27 13:07:43 2011
Backup with current user defined configuration and ibe data. Do you want to continue? (y/n)y
Connect to tftp server 172.16.1.1 ...
Please wait...
```

For improved confidence and privacy, you can protect the back up configuration file with an encryption password. This password must match when restoring the back up configuration.

```
execute backup config tftp config1.cfg 1.1.1.1
<Enter>|<passwd> Optional password to protect the backup content.
```

Related topics

restore config

user-config

backup-restore

Use these commands to back up and restore email users' mailboxes. The restored mailboxes will be merged with the current mailboxes.

Before using this command, you must first specify the schedule and storage media for backups. For details, see system backup-restore-mail on page 282.

Syntax

```
execute backup-restore all-restore
execute backup-restore check-device
execute backup-restore format-device
execute backup-restore old-restore <full_int> <incremental_int> [domain <domain_name> [user
    <user_name>]]
execute backup-restore restore {domain <domain_name> [user <user_name>] | host <host_fqdn>}
execute backup-restore start
execute backup-restore stop
```

Variable	Description	Default
all-restore	Restore mail data without deleting the previous full restore while restoring the incremental backup.	
check-device	If you use a USB device for backup, use this command to determine if the device is compatible for use with FortiMail.	
format-device	Format the backup device as preparation before a backup.	
old-restore <full_int> <incremental_int> [domain <domain_name> [user <user_name>]]	Restore mail data from a full or incremental backup identified by this FortiMail unit's FQDN, and the number of full and incremental backups. (To restore a backup from another FortiMail or a previous hostname, you must instead use `execute backup-restore restore {domain <domain_name> [user <user_name>] | host <host_fqdn>}`.) • `<full_int>`: Enter the index number of the full backup. For example, if you make a full backup each month and now have 3 full backups, then a valid value would be either `0`, `1`, or `2`. • `<incremental_int>`: Enter the index number of the incremental backup relative to the full backup. For example, if you make a full backup at the start of the month, and an incremental backup each day of the month in between full backups, then a valid value (depending on how many days are in the month) might be from `0` to `30`.	

Variable	Description	Default
	• <domain_name>: Enter the protected domain to which the mailboxes belong. If not specified, then the mailboxes of all protected domains will be restored. • <user_name>: Enter the user name whose mailbox will be restored. If not specified, then the mailboxes of all users will be restored. For details on how many full and incremental backups are available to select from, see system backup-restore-mail on page 282.	
restore {domain <domain_name> [user <user_name>] | host <host_fqdn>}	Restores mailboxes from the most recent backup. (To restore an older backup, you must instead use `execute backup-restore old-restore <full_int> <incremental_int> [domain <domain_name> [user <user_name>]]`.) • <domain_name>: Enter the protected domain to which the mailboxes belong. If not specified, then the mailboxes of all protected domains will be restored. • <user_name>: Enter the user name whose mailbox will be restored. If not specified, then the mailboxes of all users will be restored. • <host_fqdn>: Enter the FortiMail FQDN (or, if its local domain is not configured, the hostname) that was used to name the backup file. Usually, you enter the FQDN of this same FortiMail unit, but you may enter the FQDN of another FortiMail unit if you want to import mailboxes from it. For example, you may be upgrading from FortiMail A to a FortiMail B, and have a backup of the mailboxes from the FortiMail A, `fortimail.example.com`. On FortiMail B, configure it to also use the same backup storage media, then enter `fortimail.example.com` in this field to import mailboxes from FortiMail A.	
start	Immediately initiate a backup. **Caution:** All data on the backup device will be erased.	
stop	Stop any currently running backups. Time required to cancel the backup varies by the backup media, but may be up to 30 seconds.	

Related topics

restore config
backup
system backup-restore-mail

blocklist

Use this command to configure blocklist operations.

Syntax

```
execute blocklist add
execute blocklist backup
execute blocklist display on page 370
execute blocklist purge
execute blocklist remove
execute blocklist restore
```

Variable	Description	Default

add	Add a domain or user level blocklist, or system level blocklist, as shown below (respectively):
	`execute blocklist add [domain | user] <domain-name | user-name> <list-content>`
	`execute blocklist add [system] <list-content>`	

backup	Backup a domain or user level blocklist, or system level blocklist to a TFTP server, as shown below (respectively):
	`execute blocklist backup [domain | user] <domain-name | user-name> <tftp-server-ip> <file-name>`
	`execute blocklist backup [system] <tftp-server-ip> <file-name>`	

display	Dispaly a domain or user level blocklist, or system level blocklist, as shown below (respectively):
	`execute blocklist display [domain | user] <domain-name | user-name>`
	`execute blocklist display [system]`	

purge	Purge a domain or user level blocklist, or system level blocklist, as shown below (respectively):
	`execute blocklist purge [domain | user] <domain-name-list | user-name-list>`
	`execute blocklist purge [system]`	

remove	Remove a domain or user level blocklist, or system level blocklist, as shown below (respectively):
	`execute blocklist remove [domain | user] <domain-name | user-name> <list-content>`
	`execute blocklist remove [system] <list-content>`	

restore	Restore a domain or user level blocklist, or system level blocklist from a TFTP server, as shown below (respectively):
	`execute blocklist restore [domain | user] <domain-name | user-name> <tftp-server-ip> <file-name>`
	`execute blocklist restore [system] <tftp-server-ip> <file-name>`	

Related topics

safelist

certificate

Use this command to upload and download certificates, and to generate certificate signing requests (CSR).

Syntax

```
execute certificate ca import tftp <file_name> <tftp_ip>
execute certificate ca export tftp <cert_name> <file_name> <tftp_ip>
execute certificate config verify
execute certificate crl import tftp <file_name> <tftp_ip>
execute certificate crl export tftp <cert_name> <file_name> <tftp_ip>
execute certificate local export tftp <cert_name> <file_name> <tftp_ip>
execute certificate local generate <cert_name> <key_size> <subject> <country> <state>
      <organization> <unit> <email>
execute certificate local import tftp <file_name> <tftp_ip>
execute certificate local info <cert_name>
execute certificate local regenerate
execute certificate remote import tftp <file_name> <tftp_ip>
execute certificate remote export tftp <cert_name> <file_name> <tftp_ip>
```

Variable	Description	Default
ca import tftp <file_name> <tftp_ip>	Imports the certificate authority (CA) certificate from a TFTP server. Certificate authorities validate and sign other certificates in order to indicate to third parties that those other certificates may be trusted to be authentic.	
ca export tftp <cert_name> <file_name> <tftp_ip>	Exports the CA certificate to a TFTP server.	
config verify	Since FortiMail stores configuration information of CA certificates and local certificates in the configuration file and stores the certificates themselves in the file system, in some circumstances (such as a firmware upgrade or an abnormal system shutdown), the certificate configuration and the certificate may be out of sync. Use this command to synchronize the certificate configuration in the configuration file with the certificate in the file system.	
crl import tftp <file_name> <tftp_ip>	Imports the certificate revocation list (CRL). To ensure that your FortiMail unit validates only certificates that have not been revoked, you should periodically upload a current certificate revocation list, which may be provided by certificate authorities (CA). Alternatively, you can use online certificate status protocol (OCSP) to query for certificate statuses.	
crl export tftp <cert_name> <file_name> <tftp_ip>	Exports the CRL to a TFTP server.	

Variable	Description	Default
local export tftp <cert_name> <file_name> <tftp_ip>	Exports a certificate signing request or a local certificate to a TFTP server. Note that this command does not support exporting a certificate in PKCS#12 format. To do this, you must go to the web UI.	
local generate <cert_name> <key_size> <subject> <country> <state> <organization> <unit> <email>	Enter the information required to generate a certificate signing request. Certificate signing request files can then be submitted for verification and signing by a certificate authority (CA).	
local import tftp <file_name> <tftp_ip>	Imports a local certificate from a TFTP server. Note that this command does not support importing a certificate that is in PKCS#12 format. To do this, you must go to the web UI. FortiMail units require a local server certificate that it can present when clients request secure connections, including: • the web UI (HTTPS connections only) • webmail (HTTPS connections only) • secure email, such as SMTPS, IMAPS, and POP3S	
local info <cert_name>	Shows the specified certificate information.	
local regenerate	Regenerates the local self certificate.	
remote import tftp <file_name> <tftp_ip>	Imports the certificate of the online certificate status protocol (OCSP) servers of your certificate authority (CA). OCSP enables you to revoke or validate certificates by query, rather than by importing certificate revocation lists (CRL).	
remote export tftp <cert_name> <file_name> <tftp_ip>	Exports the OCSP certificate to a TFTP server.	

Related topics

profile certificate-binding

checklogdisk

Use this command to find and correct errors on the log disk.

Use this command only when recommended by Fortinet Technical Support. Logging is suspended while this command is executing.

Syntax

```
execute checklogdisk
```

Related topics

checkmaildisk

checkmaildisk

Use this command to find and correct errors on the mail disk. Actions are displayed at the command prompt. If the command cannot fix an error automatically, it displays a list of manual correction options from which you must select.

Use this command only when recommended by Fortinet Technical Support. Email-related functions are suspended while this command is executing.

Syntax

```
execute checkmaildisk
```

Related topics

checklogdisk

cleanqueue

Select to remove all messages from the deferred queue.

Syntax

```
execute cleanqueue
```

Related topics

maintain

create

This is a hidden command. Use this command to create various system-wide, domain-wide, and user-wide antispam settings.

Syntax

```
execute create custom-message <domain> <message_content>
execute create dkim-signing-key
execute create ibe-system-key <content>
execute create resource-share
execute create system-custom-message <contents>
execute create system-favicon
execute create user-auto-forward <email_addr> <content>
execute create user-auto-reply <email_addr> <content>
execute create user-calendar <user_name>
execute create user-calendar-b64
execute create user-calendar-tag <email_addr> <content>
execute create user-email-tag <email_addr> <content>
execute create user-filter-custom
execute create user-filter-master
execute create user-filter-sieve
execute create user-preference <user_name> <content>
execute create user-primaryaddr <user_name> <content>
execute create user-secondaryaddr <user_name> <content>
execute create user-signature <user_name> <content>
```

Variable	Description	Default
custom-message <domain> <message_content>	Creates domain-wide custom messages.	
dkim-signing-key	Creates DomainKeys Identified Mail (DKIM) signing key.	
resource-share	Creates a resource share.	
ibe-system-key <content>	Creates IBE system key.	
system-custom-message <contents>	Creates system-wide custom messages.	
system-favicon	Creates a system use icon file.	
user-auto-forward <email_addr> <content>	Creates an auto forward message for the user.	

Variable	Description	Default
user-auto-reply <email_addr> <content>	Creates an auto reply message for the user.	
user-calendar <user_name>	Creates a calendar for the user.	
user-calendar-b64	Creates a calendar base64 encoded.	
user-calendar-tag <email_addr> <content>	Creates a user calendar tag.	
user-email-tag <email_addr> <content>	Creates a user email tag.	
user-filter-custom	Creates a user message filter custom file.	
user-filter-master	Creates a user message filter master file.	
user-filter-sieve	Creates a user message filter sieve file.	
user-preference <user_name> <content>	Configures the user preference settings. For details, see the User chapter in the FortiMail Administration Guide.	
user-primaryaddr <user_name> <content>	Configures the primary email account for the user.	
user-secondaryaddr <user_name> <content>	Configures the secondary email account for the user.	
user-signature <user_name> <content>	Configures the email signature for the user.	

Related topics

backup

date

Use this command to set the system date.

Syntax

```
execute date <date_str>
```

Variable	Description	Default
<date_str>	Enter the system date in the format of mm/dd/yyyy.	

Related topics

system time manual
system time ntp

db

Use this command to repair, rebuild, or reset the following FortiMail databases:

- Address book
- Bayesian database
- Certificate database
- Customized messages
- Dictionaries
- DKIM key database
- Email migration database
- End point database
- End point sender reputation database
- Greylist database
- Greylist exempt database
- IBE database
- Sender reputation database
- User alias database
- User address mapping database

Syntax

```
execute db dump
execute db force-recover
execute db info
execute db rebuild
execute db reset <database>
execute db restore
execute db transfer
```

Variable	Description	Default
dump	Dumps one database file for troubleshooting.	
force-recover	Try to repair all of the databases using force recovery.	
info	Provides database information.	
rebuild	Clean and rebuild all of the databases.	

Variable	Description	Default
reset <database>	Clean and rebuild one of the FortiMail databases. <database> is one of the above-listed databases.	
restore	Restores one database.	
transfer	Transfer last dumped db file to a remote server via FTP, SCP, or TFTP. Use the following format: `execute db transfer {ftp-dump | scp-dump | tftp-dump} <file-name> <server-ip> <username> <password>`	

Related topics

maintain

dlp

Use this command to refresh the DLP fingerprints from the fingerprint server.

Syntax

```
execute dlp refresh <source_name>
```

Variable	Description	Default
<source_name>	Enter the source server address or host name.	

endpoint

Use this command to configure carrier endpoint devices. A carrier end point is any device on the periphery of a carrier's or internet service provider's (ISP) network. It could be, for example, a subscriber's GSM cellular phone, wireless PDA, or computer using DSL service.

Syntax

```
execute endpoint count
execute endpoint data backup tftp <ip_address>
execute endpoint delete <ip_address>
```

Variable	Description	Default
count	Count the total number of endpoint devices in the end point database.	
data backup tftp <ip_address>	Back up the end point database to the specified TFTP server.	
delete <ip_address>	Remove the IP address of an endpoint device from the end point database.	

erase-filesystem

Securely erases a file system by filling with random data three times.

Syntax

```
execute erase-filesystem
```

Variable	Description	Default
erase-filesystem		

factoryreset

Use this command to reset the FortiMail unit to its default settings for the currently installed firmware version. If you have not upgraded or downgraded the firmware, this restores factory default settings.

This command also erases all the log files and mail data on the hard drive.

Back up your configuration and mail data before entering this command. This procedure resets all changes that you have made to the FortiMail unit's configuration file and reverts the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the FortiMail Administration Guide.

Syntax

```
execute factoryreset
```

Example

The following example resets the FortiMail unit to default settings for the currently installed firmware version.

```
execute factoryreset
```

The CLI displays the following:

```
This operation will change all settings to
factory default! Do you want to continue? (y/n)
```

After you enter y (yes), the CLI displays the following and logs you out of the CLI:

```
System is resetting to factory default...
```

Related topics

restore config
backup

factoryreset config

Use this command to reset the system configuration to default settings.

Syntax

```
execute factoryreset config
```

Related topics

backup
factoryreset
factoryreset config2
factoryreset disk
factoryreset keeplicense
factoryreset shutdown
View a setting's default value

factoryreset config2

Use this command to reset the system configuration to default settings, while retaining the network settings and disk data.

Syntax

```
execute factoryreset config2
```

Related topics

backup
factoryreset config
factoryreset2 keeplicense

factoryreset disk

Use this command to reset the RAID level and partition disk to default settings.

Syntax

```
execute factoryreset disk
```

Related topics

backup

factoryreset keeplicense

Use this command to reset the FortiMail VM configuration to its factory default settings, but keep the VM license file.

Syntax

```
execute factoryreset keeplicense
```

Related topics

backup

factoryreset shutdown

Use this command to reset the FortiMail unit's configuration and disk partition to its factory default settings and then shutdown the system.

Syntax

```
execute factoryreset shutdown
```

Related topics

backup

factoryreset2

Use this command to reset the FortiMail unit to its default settings for the currently installed firmware version, while retaining all network settings. If you have not upgraded or downgraded the firmware, this restores factory default settings.

This command also erases all the log files and mail data on the hard drive.

Unlike `factoryreset` which resets all changes that you have made to the FortiMail unit's configuration file including its network settings, it is still recommended to back up your configuration and mail data before entering this command.

For information on creating a backup, see the FortiMail Administration Guide.

Syntax

```
execute factoryreset2
```

Example

The following example resets the FortiMail unit's configuration and disk partition to its factory default settings, while keeping the network settings.

```
execute factoryreset2
```

factoryreset2 keeplicense

Use this command to reset the FortiMail VM configuration to its factory default settings, while retaining the network settings and VM license file.

Syntax

```
execute factoryreset2 keeplicense
```

Related topics

backup

formatlogdisk

Use this command to reformat the local hard disk that contains log data.

Regularly format the hard disk to improve performance.

Back up all data on the disk before entering this command. Formatting hard disks deletes all files on that disk.

Syntax

```
execute formatlogdisk
```

Example

The following example formats the log disk.

```
execute formatlogdisk
```

The CLI displays the following:

```
This operation will erase all data on the log disk!
Do you want to continue? (y/n)
```

After you enter y (yes), the CLI displays the following and logs you out of the CLI:

```
formatting disk, Please wait a few seconds!
```

Related topics

partitionlogdisk
formatmaildisk
formatmaildisk-backup

formatmaildisk

Use this command to reformat the local hard disk that contains email data, **without** first performing a backup.

You can alternatively perform a backup before formatting the mail disk. For details, see formatmaildisk-backup on page 384.

Regularly format the hard disk to improve performance.

Back up all data on the disk before entering this command. Formatting hard disks deletes all files on that disk.

Syntax

```
execute formatmaildisk
```

Example

The following example formats the log disk.

```
execute formatmaildisk
```

The CLI displays the following:

```
This operation will erase all data on the mail disk!
Do you want to continue? (y/n)
```

After you enter y (yes), the CLI displays the following and logs you out of the CLI:

```
formatting disk, Please wait a few seconds!
```

Related topics

formatmaildisk-backup
formatlogdisk

formatmaildisk-backup

Use this command to back up data contained on the mail disk to the log disk, and then format the local mail disk.

You can alternatively format the mail disk without performing a backup. For details, see formatmaildisk on page 383.

Regularly format the hard disk to improve performance.

Syntax

```
execute formatmaildisk-backup
```

Related topics

formatmaildisk

forticloud

Use this command to manage the FortiCloud account.

Syntax

```
execute forticloud info
execute forticloud info-apt
execute forticloud join
execute forticloud login
execute forticloud sandbox-region
execute forticloud update-apt
```

Variable	Description	Default
info	Shows the FortiCloud account info if login in.	
info-apt	Show information about FortiCloud sandbox, including APT license, license expiration date, and region. DEBUG image shows cloud sandbox server IP.	
join	Joins an existing FortiCloud account. The device must be added to the account to work.	
login	Logs the user into the FortiCloud account.	
sandbox-region	Define the cloud sandbox region: • 0: Global • 1: Europe • 2: Japan • 3: US	
update-apt	Force refresh of FortiCloud sandbox server addresses.	

ha failover

Use this command to manually trigger failover in the HA cluster.

Syntax

```
execute ha failover
```

Related topics

system ha
ha restore
ha-group failover

ha hb join

Use this command to manually trigger a FortiMail unit to join an HA cluster or group of HA clusters.

Before you run this command, if HA was previously configured, you must disable it. The command will not run if HA is currently enabled.

If joining did not succeed, use `exec ha hb reset-status` to reset the HA status. Then try again.

Once the unit joins the cluster, it replaces the HA configuration (if any) in `config system ha`.

Syntax

```
execute ha hb join {<primary_ipv4> | <primary_ipv6>} {true | false} "<shared-password_str>"
    <unit-name_str> [<group_name>]
```

Variable	Description	Default
{<primary_ipv4> | <primary_ipv6>}	Enter the IP address of the primary unit in the HA cluster. (If you have a group of HA clusters, enter the IP address of the primary cluster's primary unit.)	
{true | false}	Select whether this FortiMail unit will be a primary backup. If either: • mode {active-active | active-passive} is `active-passive` • primary-backup {enable | disable} is `disable` • another unit in the cluster is already the primary backup then you should enter `false`. (`true` is ignored in those cases, because it is not valid.) Otherwise you may enter `true`. This updates the configuration in `config system ha` on the primary unit, making this secondary unit the primary backup.	
"<shared-password_str>"	Enter the password for this HA cluster. Before FortiMail units in the HA cluster synchronize with each other, they verify that they have the same password. This prevents them from accidentally synchronizing with the wrong cluster. Therefore this must match the password "<password_str>" that was configured on other units in the cluster.	
<unit-name_str>	Enter the name of this FortiMail unit in the HA cluster. This may be different from	

Variable	Description	Default
	the FQDN or hostname, in order to distinguish units in an HA cluster. This updates the configuration in `config system ha`.	
[<group_name>]	Enter the name of the group of HA clusters that you want this FortiMail unit to join. This applies only if, on the primary unit, type {group | member} is `group`. Otherwise leave it empty.	

Related topics

system ha

ha hb reset-status

ha hb reset-status

Use this command if you ran `exec ha hb join`, but it was interrupted and the unit could not successfully join the HA cluster. This clears the status so that you can attempt to join the unit to the cluster again.

Syntax

```
execute ha hb reset-status
```

Related topics

ha hb join

ha restore

Use this command to manually trigger a FortiMail unit to restore its initially configured role as secondary unit in the HA cluster.

Syntax

```
execute ha restore
```

Related topics

system ha
ha failover
ha-group restore

ha sync command config-sync-start

Use this command to manually start HA configuration synchronization.

This command does not apply to data synchronization nor to a group of HA clusters.

You must type the full command, not the abbreviated form. For example, enter:

```
exec ha sync command config-sync-start
```

not:

```
exec ha sync com config-sync-sta
```

Syntax

```
execute ha sync command config-sync-start
```

Related topics

ha hb reset-status
ha sync command config-sync-stop

ha sync command config-sync-stop

Use this command to manually stop HA configuration synchronization.

This command does not apply to data synchronization nor to a group of HA clusters.

You must type the full command, not the abbreviated form. For example, enter:

```
exec ha sync command config-sync-stop
```

not:

```
exec ha sync com config-sync-sto
```

Syntax

```
execute ha sync command config-sync-stop
```

Related topics

ha sync command config-sync-start

ha sync command failover-start

Use this command to manually enable HA failovers again after you have temporarily disabled them via `exec ha sync command failover-stop`.

You must type the full command, not the abbreviated form. For example, enter:

```
exec ha sync command failover-start
```

not:

```
exec ha sync com failover-sta
```

Syntax

```
execute ha sync command failover-start
```

Related topics

ha sync command failover-stop
ha failover
ha-group failover

ha sync command failover-stop

Use this command if you temporarily need to manually disable HA failovers.

You must type the full command, not the abbreviated form. For example, enter:

```
exec ha sync command failover-stop
```

not:

```
exec ha sync com failover-sto
```

Syntax

```
execute ha sync command failover-stop
```

Related topics

ha sync command failover-start

ha-group failover

Use this command to manually trigger failover among a group of HA clusters.

Syntax

```
execute ha-group failover
```

Related topics

system ha
ha-group restore
ha failover

ha-group restore

Use this command to manually trigger an HA cluster to restore its initially configured role as a secondary cluster in the HA group.

Syntax

```
execute ha-group restore
```

Related topics

system ha

ha-group failover
ha restore

ibe data

Use this command to generate and view an IBE data file.

Syntax

```
execute ibe data export-to-file
execute ibe data get-file-info
```

Variable	Description	Default
export-to-file	Generate an IBE data file.	
get-file-info	Get current IBE data file information.	

Related topics

db

ibe user

Use this command to maintain the expired users.

Syntax

```
execute ibe user purge-mail <user_name> <level>
execute ibe user clean-expired-user <user_name> <level>
```

Variable	Description	Default
purge-mail <user_name> <level>	Specify whose mail you want to purge/delete and also specify the verbose level.	
clean-expired-user <user_name> <level>	Specify which user you want to delete and also specify the verbose level.	

Related topics

db

license

Use this command to manage the central management license.

Syntax

```
execute license central-mgmt import tftp <ip> <file_name>
execute license central-mgmt show
```

Variable	Description	Default
import tftp <ip> <file_name>		
show	Display the license information.	

lvm

Use this command to control the logical volume manager (LVM) support on the FortiMail-VM platforms.

Since this feature is added in 5.2.0 release, if you're upgrading from older FortiMail-VM releases to 5.2.0 release, LVM is not enabled by default. If you want to enable it, you must be aware that all the mail data and log data will be erased.

Syntax

```
execute lvm disable
execute lvm enable <percentage>
execute lvm extend <percentage>
execute lvm summary
```

Variable	Description	Default
disable	Stop LVM on the system.	
enable <percentage>	Start LVM on the system. Also specify how much percent of the hard disk space will be allocated to the log disk. The remaining will be assigned to the mail disk. If not specified, the default percentage is 20.	enable (for new install) 20

Variable	Description	Default
extend <percentage>	Use this command to add new drives to the system. See above for the usage of percentage.	20
summary	Displays the LVM status and details.	

maintain

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

Syntax

```
execute maintain mailqueue clear age <time_str>
```

Variable	Description	Default
age <time_str>	Enter an age between 1 hour and 10 years. The FortiMail unit deletes mail messages in the mail queues greater than this age. The age consists of an integer appended to a letter that indicates the unit of time: `h` (hours), `d` (days), `m` (months), or `y` (years).	24h

Example

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

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

The CLI would display the following message:

Clearing messages in mail queues at least 23 days old.

Related topics

cleanqueue

nslookup

Use this command to query the DNS server for domain name or IP address mapping or for any other specific DNS record.

Syntax

```
execute nslookup name <fqdn | ip> type <type> class <class> server <dns_server> port <port_
    number>
```

Variable	Description	Default
name <fqdn | ip> type <type> class <class> server <dns_server> port <port_number>	<fqdn | ip>: enter either an IP address or a fully qualified domain name (FQDN) of a host. <type>: optionally specify the DNS query type: A -- host address AAAA -- IPv6 address ANY -- all cached records CNAME -- canonical name DLV -- DNSSEC lookaside validation DNSKEY -- DNS key DS -- delegation signer MX -- mail exchanger NS -- authoritative name server NSEC -- next SECure NSEC3 -- NSEC3 parameters PTR -- domain name pointer RRSIG -- DNSSEC signature SOA -- start of authority zone SPF -- sender policy framework TA -- DNSSEC trust authorities TXT -- text string The default type is A. <class>: optionally specify the DNS class type: either IN or ANY. <dns_server>: optionally specify the DNS server's host name or IP address. If you do not specify the server here, FortiMail will use its local host DNS settings. <port_number>: optionally specify the port number of the DNS server.	A ANY 53

Example

You could use this command to determine the DNS resolution for the fully qualified domain name mail.example.com

```
execute nslookup name mail.example.com
```

The CLI would display the following:

```
Name: example.com
Address: 192.168.1.15
```

Similarly, you could use this command to determine the domain name hosted on the IP address 192.168.1.15:

```
execute nslookup name 192.168.1.15 type ptr
```

The CLI would display the following:

```
Address: 192.168.1.15
Name: mail.example.com
```

You could also use this command to determine the host that is mail exchanger (MX) for the domain example.com:

```
execute nslookup name example.com type mx
```

The CLI would display the following:

```
example.com mail exchanger = 10 mail.example.com.
```

Related topics

ping
traceroute
system dns

partitionlogdisk

Use this command to adjust the size ratio of the hard disk partitions for log and mail data.

Back up all data on the disks before beginning this procedure. Partitioning the hard disks deletes all files on those disks.

Syntax

```
execute partitionlogdisk <logpercentage_str>
```

Variable	Description	Default
partitionlogdisk <logpercentage_str>	Enter an integer between 10 and 90 to create a partition for log files using that percentage of the total hard disk space. The remaining partition (by default, 75% of the hard disk space) will be used for mail data.	20

Related topics

formatlogdisk

ping

Use this command to perform an ICMP ECHO request (also called a ping) to a host by specifying its fully qualified domain name (FQDN) or IP address, using the options configured by ping-option on page 397.

Pings are often used to test connectivity.

Syntax

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

Variable	Description	Default
ping {<fqdn_str> | <host_ipv4>}	Enter either the IP address or fully qualified domain name (FQDN) of the host.	

Example

This example pings a host with the IP address 172.16.1.10.

```
execute ping 172.16.1.10
```

The CLI displays the following:

```
PING 172.16.1.10 (172.16.1.10): 56 data bytes
      64 bytes from 172.16.1.10: icmp_seq=0 ttl=128 time=0.5 ms
      64 bytes from 172.16.1.10: icmp_seq=1 ttl=128 time=0.2 ms
      64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=0.2 ms
      64 bytes from 172.16.1.10: icmp_seq=3 ttl=128 time=0.2 ms
      64 bytes from 172.16.1.10: icmp_seq=4 ttl=128 time=0.2 ms
--- 172.16.1.10 ping statistics ---
      5 packets transmitted, 5 packets received, 0% packet loss
      round-trip min/avg/max = 0.2/0.2/0.5 ms
```

The results of the ping indicate that a route exists between the FortiMail unit and 172.16.1.10. It also indicates that during the sample period, there was no packet loss, and the average response time was 0.2 milliseconds (ms).

Example

This example pings a host with the IP address 10.0.0.1.

```
execute ping 10.0.0.1
```

The CLI displays the following:

```
PING 10.0.0.1 (10.0.0.1): 56 data bytes
```

After several seconds, no output has been displayed. The administrator halts the ping by pressing Ctrl + C. The CLI displays the following:

```
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

The results of the ping indicate that the host may be down, or that there is no route between the FortiMail unit and 10.0.0.1. To determine the cause, further diagnostic tests are required, such as traceroute on page 412.

Related topics

ping-option
smtptest
telnettest
traceroute
system dns

ping-option

Use this command to configure behavior of ping on page 396.

Syntax

```
execute ping-option data-size <bytes_int>
execute ping-option df-bit {yes | no}
execute ping-option pattern <bufferpattern_hex>
execute ping-option repeat-count <repeat_int>
execute ping-option source {auto | <interface_ipv4>}
execute ping-option timeout <seconds_int>
execute ping-option tos {default | lowcost | lowdelay | reliability | throughput}
execute ping-option ttl <hops_int>
execute ping-option validate-reply {yes | no}
execute ping-option view-settings
```

Variable	Description	Default
data-size <bytes_int>	Enter datagram size in bytes.This allows you to send out packets of different sizes for testing the effect of packet size on the connection. If you want to configure the pattern that will be used to buffer small datagrams to reach this size, also configure `pattern <bufferpattern_hex>`.	56

Variable	Description	Default
df-bit {yes | no}	Enter either `yes` to set the DF bit in the IP header to prevent the ICMP packet from being fragmented, or enter `no` to allow the ICMP packet to be fragmented.	no
pattern <bufferpattern_hex>	Enter a hexadecimal pattern, such as `00ffaabb`, to fill the optional data buffer at the end of the ICMP packet. The size of the buffer is determined by `data-size <bytes_int>`.	
repeat-count <repeat_int>	Enter the number of times to repeat the ping.	5
source {auto | <interface_ipv4>}	Select the network interface from which the ping is sent. Enter either `auto` or a mail network interface's IP address.	auto
timeout <seconds_int>	Enter the ping response timeout in seconds.	2
tos {default | lowcost | lowdelay | reliability | throughput}	Enter the IP type-of-service option value, either: • `default`: Do not indicate (that is, set the TOS byte to 0). • `lowcost`: Minimize cost. • `lowdelay`: Minimize delay. • `reliability`: Maximize reliability. • `throughput`: Maximize throughput.	default
ttl <hops_int>	Enter the time-to-live (TTL) value.	64
validate-reply {yes | no}	Select whether or not to validate ping replies.	no
view-settings	Display the current ping option settings.	

Example

This example sets the number of pings to three and the source IP address to that of the port2 network interface, 10.10.10.1, then views the ping options to verify their configuration.

```
execute ping-option repeat-count 3
execute ping-option source 10.10.10.1
execute ping-option view-settings
```

The CLI would display the following:

```
Ping Options:
Repeat Count: 3
Data Size: 56
Timeout: 2
TTL: 64
TOS: 0
DF bit: unset
Source Address: 10.10.10.1
Pattern:
Pattern Size in Bytes: 0
Validate Reply: no
```

Related topics

ping
traceroute

ping6

Use this command to perform a ping6 request to an IPv6 host by specifying its fully qualified domain name (FQDN) or IP address, using the options configured by ping6-option on page 399.

Pings are often used to test connectivity.

Syntax

```
execute ping6 {<fqdn_str> | <host_ipv4>}
```

Variable	Description	Default
ping6 {<fqdn_str> | <host_ipv4>}	Enter either the IP address or fully qualified domain name (FQDN) of the host.	

Related topics

ping
ping6-option

ping6-option

Use this command to configure behavior of ping6 on page 399.

Syntax

```
execute ping6-option data-size <bytes_int>
execute ping6-option pattern <bufferpattern_hex>
execute ping6-option repeat-count <repeat_int>
execute ping6-option source {auto |  <interface_ipv4>}
execute ping6-option timeout <seconds_int>
execute ping6-option tos {default | lowcost | lowdelay | reliability | throughput}
execute ping6-option ttl <hops_int>
```

```
execute ping6-option validate-reply {yes | no}
execute ping6-option view-settings
```

Variable	Description	Default
data-size <bytes_int>	Enter datagram size in bytes.This allows you to send out packets of different sizes for testing the effect of packet size on the connection. If you want to configure the pattern that will be used to buffer small datagrams to reach this size, also configure `pattern <bufferpattern_hex>`.	56
pattern <bufferpattern_hex>	Enter a hexadecimal pattern, such as `00ffaabb`, to fill the optional data buffer at the end of the ICMP packet. The size of the buffer is determined by `data-size <bytes_int>`.	
repeat-count <repeat_int>	Enter the number of times to repeat the ping.	5
source {auto | <interface_ipv4>}	Select the network interface from which the ping is sent. Enter either `auto` or a mail network interface's IP address.	auto
timeout <seconds_int>	Enter the ping response timeout in seconds.	2
tos {default | lowcost | lowdelay | reliability | throughput}	Enter the IP type-of-service option value, either: • `default`: Do not indicate (that is, set the TOS byte to 0). • `lowcost`: Minimize cost. • `lowdelay`: Minimize delay. • `reliability`: Maximize reliability. • `throughput`: Maximize throughput.	default
ttl <hops_int>	Enter the time-to-live (TTL) value.	64
validate-reply {yes | no}	Select whether or not to validate ping replies.	no
view-settings	Display the current ping option settings.	

Related topics

ping
ping6
db

raid

Use this command to find and add a hard disk to the array unit after you insert a second hard disk into the drive bay.

This command is only available for some FortiMail platforms which support RAID.

Syntax

```
execute raid add-disk
```

Example

You could notify the RAID controller to add the hard disk to the array unit after inserting a new hard disk.

```
execute raid
```

The CLI displays the following:

```
This operation will scan for new hard drives and add them into the RAID array
Do you want to continue? (y/n)
```

After you enter y (yes), if all hard disks have already been added to an array, the CLI displays the following:

```
existing raid disk at 12 is 120034123776
existing raid disk at 13 is 120034123776
no NEW disks in the system
```

Related topics

system status

reboot

Use this command to restart the FortiMail unit.

Syntax

```
execute reboot
```

Example

The following example reboots the FortiMail unit.

```
execute reboot
```

The CLI displays the following:

```
This operation will reboot the system !
Do you want to continue? (y/n)
```

After you enter y (yes), the CLI displays the following:

```
System is rebooting...
```

If you are connected to the CLI through a local console, the CLI displays messages while the reboot is occurring.

If you are connected to the CLI through the network, the CLI will not display any notification while the reboot is occurring, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection is terminated. Time required by the reboot varies by many factors, such as whether or not hard disk verification is required, but may be several minutes.

Related topics

shutdown

reload

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

In addition, you can also use this command to reload individual daemons that have crashed. In this case, the command is as following:

```
execute reload [{httpd | ...}]
```

where `[{httpd | ...}]` indicates the name of a specific daemon that you want to restart, if you want to limit the reload to a specific daemon.

For example, if HTTP and HTTPS access are enabled, but you cannot get a connection response on webmail or the GUI, although you can still connect via SSH and ping. Thus you know that the FortiMail unit has not crashed entirely. If you do not want to reboot because this would interrupt SMTP, you can choose to restart the HTTP daemon only.

```
FortiMail-400 # execute reload httpd
Restart httpd?
Do you want to continue? (y/n)y

Reloading httpd....done
```

Note that the command does not check whether your indicated daemon actually exists. It simply indicates whether the command is executed. If the command does not take a few seconds to execute, it is possible that the daemon does not really exist.

Syntax

```
execute reload [<daemon_name>]
```

Related topics

- reboot
- restore config
- restore image

restore as

Use this command to restore an antispam configuration file from a TFTP server.

Syntax

```
execute restore as tftp <filename_str> <server_ipv4>
```

Variable	Description	Default
<filename_str>	Enter the name of the configuration file stored on a TFTP server.	
<server_ipv4>	Enter the IP address of the TFTP server where the configuration file is stored.	

Related topics

- restore av

restore av

use this command to restore an antivirus configuration file from a TFTP server.

Syntax

```
execute restore av tftp <filename_str> <server_ipv4>
```

Variable	Description	Default
<filename_str>	Enter the name of the configuration file stored on a TFTP server.	
<server_ipv4>	Enter the IP address of the TFTP server where the configuration file is stored.	

Related topics

restore as

restore config

Use this command to restore a primary configuration file from a TFTP server.

Back up your configuration before entering this command. This procedure can perform large changes to your configuration, including, if you are downgrading the firmware, resetting all changes that you have made to the FortiMail unit's configuration file and reverting the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the FortiMail Administration Guide.

Unlike installing firmware via TFTP during a boot interrupt, installing firmware using this command will attempt to preserve settings and files, and not necessarily restore the FortiMail unit to its firmware/factory default configuration. For information on installing firmware via TFTP boot interrupt, see the FortiMail Administration Guide.

Syntax

```
execute restore config {tftp <filename_str> <server_ipv4> |
      management-station {normal | template} <revision_int>}
```

Variable	Description	Default
<filename_str>	If you want to restore a configuration file stored on a TFTP server, enter the name of the configuration file.	
<server_ipv4>	If you want to restore a configuration file stored on a TFTP server, enter the IP address of the TFTP server.	
management-station {normal | template}	If you want to restore a configuration file or apply a template stored on a FortiManager unit, enter the `management-station` keyword then enter either: • `normal`: Restore a configuration revision number. • `template`: Apply a template revision number.	
<revision_int>	If you want to restore a configuration file or apply a template stored on a FortiManager unit, enter the revision number of the configuration file or template.	

Example

This example restores configuration file revision 2, which is stored on the FortiManager unit.

```
execute restore config management-station normal 2
```

The CLI displays the following:

```
This operation will overwrite the current settings!
Do you want to continue? (y/n)
```

After you enter y (yes), the CLI displays the following:

```
Connect to FortiManager ...
Please wait...
```

Example

This example restores a configuration file from a TFTP server at 172.16.1.5.

```
execute restore config tftp fml.cfg 172.16.1.5
```

The CLI displays the following:

```
This operation will overwrite the current settings!
(The current admin password will be preserved.)
Do you want to continue? (y/n)
```

After you enter y (yes), the CLI displays the following, then terminates the SSH connection and reboots with the restored configuration:

```
Connect to tftp server 172.16.1.5 ...
Please wait...

Get config file from tftp server OK.
File check OK.
```

Related topics

backup

restore image

Use this command to restore a firmware file from an FTP, SCP (SSH or SFTP), or TFTP server.

Back up your configuration before entering this command. This procedure can perform large changes to your configuration, including, if you are downgrading the firmware, resetting all changes that you have made to the FortiMail unit's configuration file and reverting the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the FortiMail Administration Guide.

Syntax

```
execute restore image {ftp|scp|tftp <filename_str> <server_ipv4> <username_str> <password_str>
```

Variable	Description	Default
<filename_str>	Enter the name of the firmware file backup file.	
<server_ipv4>	Enter the IP address of the server.	
<username_str> <password_str>	If the server requires a username and password, enter them.	

Example

This example restores firmware file FE_2000A-v300-build397-FORTINET.out, which is stored on the TFTP server 192.168.1.20.

```
execute restore image tftp FE_2000A-v300-build397-FORTINET.out 192.168.1.20
```

The CLI displays the following:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

After you enter y (yes), the CLI displays the following:

```
Connect to tftp server 192.168.1.20 ...
Please wait...
########################
Get image from tftp server OK.
Check image OK.
```

Related topics

restore config

system status

restore mail-queues

Use this command to restore a mail queue file from a TFTP server.

Back up your configuration before entering this command. This procedure can perform large changes to your configuration, including, if you are downgrading the firmware, resetting all changes that you have made to the FortiMail unit's configuration file and reverting the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the FortiMail Administration Guide.

Syntax

```
execute restore mail-queues {tftp <filename_str> <server_ipv4>}
```

Variable	Description	Default
<filename_str>	If you want to restore a firmware file stored on a TFTP server, enter the name of the firmware file backup file.	
<server_ipv4>	If you want to restore a firmware file stored on a TFTP server, enter the IP address of the TFTP server.	

Related topics

restore config

safelist

Use this command to configure safelist operations.

Syntax

```
execute safelist add
execute safelist backup
execute safelist display
execute safelist purge
execute safelist remove
execute safelist restore
```

Variable	Description	Default

add	Add a domain or user level safelist, or system level safelist, as shown below (respectively):
	`execute safelist add [domain | user] <domain-name | user-name> <list-content>`
	`execute safelist add [system] <list-content>`	

backup	Backup a domain or user level safelist, or system level safelist to a TFTP server, as shown below (respectively):
	`execute safelist backup [domain | user] <domain-name | user-name> <tftp-server-ip> <file-name>`
	`execute safelist backup [system] <tftp-server-ip> <file-name>`	

display	Dispaly a domain or user level safelist, or system level safelist, as shown below (respectively):
	`execute safeist display [domain | user] <domain-name | user-name>`
	`execute safelist display [system]`	

purge	Purge a domain or user level safelist, or system level safelist, as shown below (respectively):
	`execute safelist purge [domain | user] <domain-name-list | user-name-list>`
	`execute safelist purge [system]`	

remove	Remove a domain or user level safelist, or system level safelist, as shown below (respectively):
	`execute safelist remove [domain | user] <domain-name | user-name> <list-content>`
	`execute safelist remove [system] <list-content>`	

restore	Restore a domain or user level safelist, or system level safelist from a TFTP server, as shown below (respectively):
	`execute safelist restore [domain | user] <domain-name | user-name> <tftp-server-ip> <file-name>`
	`execute safelist restore [system] <tftp-server-ip> <file-name>`	

Related topics

blocklist

sched-backup

Use this command to schedule backup to FortiManager.

Syntax

```
execute sched-backup
```

shutdown

Use this command to prepare the FortiMail unit to be powered down by halting the software, clearing all buffers, and writing all cached data to disk.

Power off the FortiMail unit only after issuing this command. Unplugging or switching off the FortiMail unit without issuing this command could result in data loss.

Syntax

```
execute shutdown
```

Example

The following example halts the FortiMail unit.

```
execute shutdown
```

The CLI displays the following:

```
This operation will halt the system
(power-cycle needed to restart)!Do you want to continue? (y/n)
```

After you enter y (yes), the CLI displays the following:

```
System is shutting down...(power-cycle needed to restart)
```

If you are connected to the CLI through a local console, the CLI displays a message when the shutdown is complete.

If you are connected to the CLI through the network, the CLI will not display any notification when the shutdown is complete, as this occurs after the network interfaces have been shut down. Instead, you may notice that the connection times out.

Related topics

reboot

smtptest

Use this command to test SMTP connectivity to a specified host.

Syntax

```
execute smtptest {<fqdn_str> | <host_ipv4>}[:<port_int>] [domain <domain_str>]
```

Variable	Description	Default
{<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the SMTP server.	
[:<port_int>]	If the SMTP server listens on a port number other than port 25, enter a colon (:) followed by the port number.	:25
[domain <domain_str>]	If you want to test the connection from an IP address in the protected domain's IP pool, enter the name of the protected domain.	

Example

This example tests the connection to an SMTP server at 192.168.1.10 on port 2525. For the outgoing connection, the FortiMail unit uses the source IP address 192.168.1.20 from the IP pool selected in the protected domain example.com.

```
execute smtptest 192.168.1.10:2525 domain example.com
```

The CLI displays the following:

```
(using 192.168.1.20 to connect)
Remote Output:
220 fortimail.example.com ESMTP Smtpd; Mon, 19 Jan 2009
 13:27:35 -0500
Connection Status:
Connecting to remote host succeeded.
```

Related topics

telnettest
traceroute
ping

system dns

ssh

Use this command to connect to another device via SSH.

Syntax

```
execute ssh <username@host> <password>
```

Variable	Description	Default
<username@host> <password>	Enter the user name and password. The host can be an IP address or the host name of the remote device.	

storage

Use this command to configure remote file storage.

Syntax

```
execute storage format
execute storage fscheck
execute storage start
execute storage test
```

Variable	Description	Default
format	Remove all data on the remote storage device.	
fscheck	Check the remote file storage system.	
start	Start the remote storage daemon.	
test	Test the remote file storage system.	

telnettest

Use this command to test Telnet connectivity to a specified host.

Syntax

```
execute telnettest {<fqdn_str> | <host_ipv4>}[:<port_int>]
```

Variable	Description	Default
{<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the Telnet server.	
[:<port_int>]	If the Telnet server listens on a port number other than port 23, enter a colon (:) followed by the port number.	:23

Example

This example tests the connection to an Telnet server at 192.168.1.10 on port 2323.

```
execute telnettest 192.168.1.10:2323
```

The CLI displays the following:

```
(using 192.168.1.20 to connect)
Remote Output(hex):
FF FD 18 FF FD 20 FF FD
23 FF FD 27
Connection Status:
Connecting to remote host succeeded.
```

Related topics

smtptest
traceroute
ping
system dns

traceroute

Use this command to use ICMP to test the connection between the FortiMail unit and another network device, and display information about the time required for network hops between the device and the FortiMail unit.

Syntax

```
execute traceroute {<fqdn_str> | <host_ipv4>}
```

Variable	Description	Default
traceroute {<fqdn_str> | <host_ipv4>}	Enter the IP address or fully qualified domain name (FQDN) of the host.	

Example

This example tests connectivity between the FortiMail unit and http://docs.fortinet.com. In this example, the trace times out after the first hop, indicating a possible connectivity problem at that point in the network.

```
FortiMail# execute traceoute docs.fortinet.com
traceroute to docs.fortinet.com (65.39.139.196), 30 hops max, 38 byte packets
 1  172.16.1.200 (172.16.1.200) 0.324 ms 0.427 ms 0.360 ms
2  * * *
```

Example

This example tests the availability of a network route to the server example.com.

```
execute traceroute example.com
```

The CLI displays the following:

```
traceroute to example.com (192.168.1.10), 32 hops max, 72 byte packets
 1 172.16.1.2   0 ms 0 ms 0 ms
 2  10.10.10.1  <static.isp.example.net> 2 ms 1 ms 2 ms
 3  10.20.20.1   1 ms   5 ms  1 ms
 4  10.10.10.2  <core.isp.example.net> 171 ms 186 ms 14 ms
 5  10.30.30.1  <isp2.example.net> 10 ms 11 ms 10 ms
 6  10.40.40.1  73 ms 74 ms 75 ms
 7 192.168.1.1  79 ms 77 ms 79 ms
 8 192.168.1.2 73 ms 73 ms 79 ms
 9 192.168.1.10 73 ms 73 ms 79 ms
10 192.168.1.10 73 ms 73 ms 79 ms
```

Example

This example attempts to test connectivity between the FortiMail unit and example.com. However, the FortiMail unit could not trace the route, because the primary or secondary DNS server that the FortiMail unit is configured to query could not resolve the FQDN `example.com` into an IP address, and it therefore did not know to which IP address it should connect. As a result, an error message is displayed.

```
FortiMail# execute traceroute example.com
traceroute: unknown host example.com
Command fail. Return code 1
```

To resolve the error message in order to perform connectivity testing, the administrator would first configure the FortiMail unit with the IP addresses of DNS servers that are able to resolve the FQDN `example.com`. For details, see system dns on page 293.

Related topics

- smtptest
- telnettest
- ping
- ping-option
- system dns

update

Use this command to manually request updates to the FortiGuard Antivirus and FortiGuard Antispam engine and definitions from the FortiGuard Distribution Network (FDN).

You can alternatively or additionally configure scheduled updates and push updates. For details, see system fortiguard antivirus on page 299 and system fortiguard antispam on page 302.

Syntax

```
execute update {as | av | now}
```

Related topics

- system fortiguard antivirus
- system fortiguard antispam
- system status

user-config

Use this command to generate a file with the latest user-specific configurations, such as user preferences, personal block/safelists, and secondary addresses, to the user configuration file, so that you will have the latest configuration when you make a configuration backup using backup.

Syntax

```
execute user-config generate
execute user-config getinfo
```

Variable	Description	Default
generate	Updates the user configuration file with the latest user-specific configuration.	
getinfo	Displays the time stamp when the last configuration file update was performed.	

Related topics

backup

vm

Every Fortinet VM includes a 15-day trial license. During this time the FortiMail VM operates in evaluation mode.

Before using the FortiMail VM you must activate it by installing a valid license.

Depending how your FortiMail VM is licensed, there two ways to you can install the license and activate the VM:

- If you get the license file from Fortinet Customer Service & Support portal upon registration, you can fetch the license file from the server where it is stored and install it.
- Starting from v7.6.2, FortiMail supports FortiFex tokens. FortiFlex (formerly Flex-VM) is a subscription service to configure and manage VM usage entitlements. Subscribers can create multiple sets of a single VM entitlement that corresponds to a licensed virtual machine. Each entitlement contains a base VM and one service bundle. Usage entitlements require a unique token to be installed on every VM. Once the VM configurations are defined and VM entitlements are created in the FortiFlex portal, a token is also generated. For details, see the FortiFlex documentation. Then you can enter the token as described below.

Syntax

```
execute vm license <filename> {ftp | scp | tftp} on page 415
execute vm forticare-license <token> on page 415
```

Variable	Description	Default
license <filename> {ftp | scp | tftp}	Specify the license file name and the storage server IP address.	
forticare-license <token>	Enter the FortiFlex token you copied from the FortiFlex portal.	

get

`get` commands display a part of your FortiMail unit's configuration in the form of a list of settings and their values.

Unlike `show`, `get` displays **all** settings, even if they are still in their default state.

For example, you might get the current DNS settings:

```
FortiMail# get system dns
primary : 172.16.95.19
secondary : 0.0.0.0
private-ip-query : enable
cache : enable
```

Notice that the command displays the setting for the secondary DNS server, even though it has not been configured, or has been reverted to its default value.

Also unlike `show`, unless used from within an object or table, `get` requires that you specify the object or table whose settings you want to display.

For example, at the root prompt, this command would be valid:

```
FortiMail# get system dns
```

and this command would not:

```
FortiMail# get
```

Depending on whether or not you have specified an object, like `show`, `get` may display one of two different outputs: either the configuration that you have just entered but not yet saved, or the configuration as it currently exists on the disk, respectively.

For example, immediately after configuring the secondary DNS server setting but **before** saving it, `get` displays two different outputs (differences highlighted in bold):

```
FortiMail# config system dns
(dns)# set secondary 192.168.1.10
(dns)# get
primary : 172.16.95.19
secondary : 192.168.1.10
private-ip-query : enable
cache : enable
(dns)# get system dns
primary : 172.16.95.19
secondary : 0.0.0.0
private-ip-query : enable
cache : enable
```

The first output from `get` indicates the value that you have configured but not yet saved; the second output from `get` indicates the value that was last saved to disk.

If you were to now enter `end`, saving your setting to disk, `get` output for both syntactical forms would again match. However, if you were to enter `abort` at this point and discard your recently entered secondary DNS setting instead of saving it to disk, the FortiMail unit's configuration would therefore match the second output, not the first.

If you have entered settings but cannot remember how they differ from the existing configuration, the two different forms of `get`, with and without the object name, can be a useful way to remind yourself.

Most `get` commands, such as `get system dns`, are used to display configured settings. You can find relevant information about such commands in the corresponding config commands in the `config` chapter.

Other `get` commands, such as `system performance`, are used to display system information that is **not** configurable. This chapter describes this type of `get` command.

Although not explicitly shown in this section, for all config commands, there are related `get` and show & show full-configuration commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see config.

system performance

Displays the FortiMail unit's CPU usage, memory usage, system load, and up time.

Syntax

```
get system performance
```

Example

```
FortiMail# get system performance
CPU usage: 0% used, 100% idle
Memory usage: 17% used
System Load: 5
Uptime: 0 days, 8 hours, 24 minutes.
```

Related topics

system status

system status

Use this command to display FortiMail system status information including:

- firmware version, build number, and date
- serial number
- BIOS version
- VM license registration and validation status (FortiMail-VM only)
- log hard disk availability
- mailbox disk availability
- file system mode (for example, `Read-Write`)
- host name
- operation mode
- high availability (HA) mode and role
- strong encryption status
- distribution scope (for example, `International`)
- FortiGuard package versions (for example, the FortiGuard Antivirus signature database)
- certificate bundle
- uptime
- system time

Syntax

```
get system status
```

Example

```
Version: FortiMail-VM v7.6.2, build753, 2024.11.27 (Debug)
Architecture: 64-bit
Serial-Number: FEVMxxxxxxxxxxx
BIOS version: n/a
VM Registration: Valid: License has been authorized
VM License File: License file and resources are valid
VM Resources: 1 CPU/8 allowed, 3952 MB RAM, 4096 MB maximum, 1048576 MB allowed, 249 GB Disk/8192 GB
      allowed
Log disk: Capacity 49 GB, Used 1220 MB (2.41%), Free 48 GB
Mailbox disk: Capacity 198 GB, Used 408 MB (0.21%), Free 197 GB
Filesystem mode: Read-Write
Hostname: FEVM080000216197
Operation mode: Server
HA type: Off
HA member mode: Off
HA member role: configured: Off; effective: Off
Strong-crypto: enabled
Distribution: International
```

```
Branch point: 753
Virus DB: 92.09335(2024-12-06 07:39)
Extended DB: Disabled
AntiSpam DB: 7.00626(2024-11-25 21:24)
GeoIP DB: 2.00258(2024-12-03 14:02)
Certificate Bundle: 1.00053(2024-11-26 15:00)
Uptime: 7 days 22 hours 42 minutes
Last reboot: Thu Nov 28 10:10:41 PST 2024
System time: Fri Dec 06 08:53:40 PST 2024
```

Related topics

- system performance
- restore image
- system global
- system ha
- system mailserver
- system security crypto
- update
- formatlogdisk
- formatmaildisk
- profile antispam
- profile antivirus

show & show full-configuration

The `show` commands display a part of your FortiMail unit's configuration in the form of commands that are required to achieve that configuration from the firmware's default state.

Although not explicitly shown in this section, for all config commands, there are related get and `show` commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see the `config` chapters.

Unlike `get`, `show` does **not** display settings that are assumed to remain in their default state.

For example, you might show the current DNS settings:

```
FortiMail# show system dns
config system dns
   set primary 172.16.1.10
end
```

Notice that the command does **not** display the setting for the secondary DNS server. This indicates that it has not been configured, or has reverted to its default value.

Exceptions include `show full-configuration` commands. This displays the full configuration, **including** the default settings, similar to `get` commands. However, `show full-configuration` output uses configuration file syntax, while `get` commands do not.

For example, you might show the current DNS settings, **including** settings that remain at their default values (differences highlighted in bold):

```
FortiMail# show full-configuration system dns
config system dns
   set primary 172.16.1.10
   set secondary 172.16.1.11
   set private-ip-query disable
   set cache enable
end
```

Depending on whether or not you have specified an object, like `get`, `show` may display one of two different outputs: either the configuration that you have just entered but not yet saved, or the configuration as it currently exists on the disk, respectively.

For example, immediately after configuring the secondary DNS server setting but **before** saving it, `show` displays two different outputs (differences highlighted in bold):

```
FortiMail# config system dns
FortiMail (dns)# set secondary 192.168.1.10
FortiMail (dns)# show
config system dns
   set primary 172.16.1.10
   set secondary 192.168.1.10
   set private-ip-query enable
   set cache enable
end
```

```
FortiMail (dns)# show system dns
config system dns
   set primary 172.16.1.10
end
```

The first output from `show` indicates the value that you have configured but not yet saved; the second output from `show` indicates the value that was last saved to disk.

If you have entered settings but cannot remember how they differ from the existing configuration, the two different forms of `show`, with and without the object name, can be a useful way to remind yourself.

If you were to now enter `end`, saving your setting to disk, `show` output for both syntactical forms would again match. However, if you were to enter `abort` at this point and discard your recently entered secondary DNS setting instead of saving it to disk, the FortiMail unit's configuration would therefore match the second output, not the first.

CLI Reference

FortiMail 7.6.2