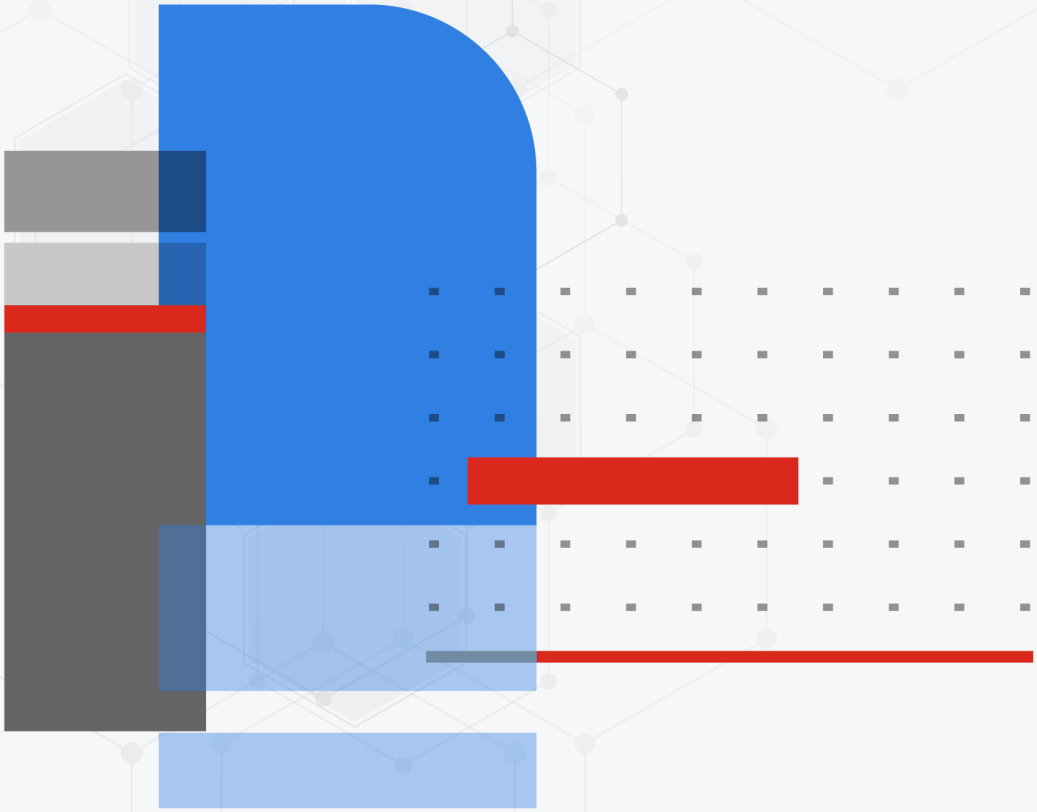
# CLI Reference

FortiMail 7.2.4



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

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

**FORTINET BLOG**
https://blog.fortinet.com

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

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

**NSE INSTITUTE**
https://training.fortinet.com

**FORTIGUARD CENTER**
https://www.fortiguard.com

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

**FEEDBACK**
Email: techdoc@fortinet.com

May 18, 2023
FortiMail 7.2.4 CLI Reference
06-724-000000-20230518

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| 2023-05-18 | Initial release. |

# Using the CLI

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

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

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

This section contains the following topics:



## Connecting to the CLI

You can access the CLI in two ways:

- Locally — Connect your computer directly to the FortiMail unit's console port.
- Through the network — Connect your computer through any network attached to one of the FortiMail unit's network ports. The network interface must have enabled Telnet or 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 web UI. 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 (see the following procedure)
- the web manager (see the *FortiMail Administration Guide*)

### 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 19.

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 256.

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

If four (three for FortiWeb) 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 documentation uses the following conventions to describe valid command syntax.

**See also**

Using the CLI on page 18

## Terminology

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

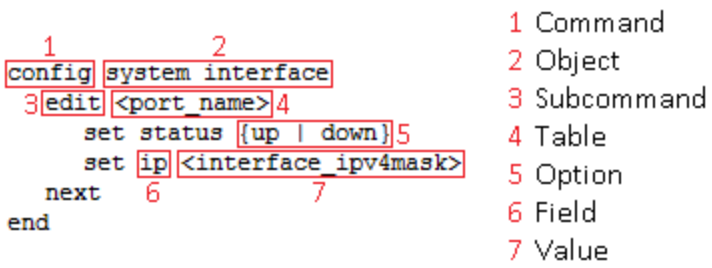
```
get system admin
```

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

```
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 35).

  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 on page 24

Notation on page 26

## 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:<br>`[verbose {1 \| 2 \| 3}]`<br>indicates that you may either omit or type both the `verbose` word and its accompanying option, such as:<br>`verbose 3` |
| Angle brackets `< >` | A word constrained by data type.<br>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:<br>`<retries_int>`<br>indicates that you should enter a number of retries, such as `5`.<br>Data types include:<br>• `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`.<br>• `<xxx_index>`: An index number referring to another part of the configuration, such as `0` for the first static route.<br>• `<xxx_pattern>`: A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`. If the pattern does not, for example, accept regular expressions, but requires wild cards only, note that in the Description column.<br>• `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`. |

| Convention | Description |
|---|---|
| | • <xxx_email>: An email address, such as admin@mail.example.com.<br>• <xxx_url>: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as http://www.fortinet./com/.<br>• <xxx_ipv4>: An IPv4 address, such as 192.168.1.99.<br>• <xxx_v4mask>: A dotted decimal IPv4 netmask, such as 255.255.255.0.<br>• <xxx_ipv4mask>: A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0.<br>• <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.<br>• <xxx_ipv4range>: A hyphen ( - ) delimited inclusive range of IPv4 addresses, such as 192.168.1.1-192.168.1.255.<br>• <xxx_ipv6>: A colon( : )-delimited hexadecimal IPv6 address, such as 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234.<br>• <xxx_v6mask>: An IPv6 netmask, such as /96.<br>• <xxx_ipv6mask>: An IPv6 address and netmask separated by a space.<br>• <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.<br>• <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.<br>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:<br>{enable \| disable}<br>indicates that you must enter either enable or disable, but must not enter both. |
| Options delimited by spaces | Non-mutually exclusive options. For example:<br>{http https ping snmp ssh telnet}<br>indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as:<br>ping https ssh<br>**Note**: To change the options, you must re-type the entire list. For example, to add snmp to the previous example, you would type:<br>ping https snmp ssh<br>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 on page 26

Terminology on page 24

# 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.<br>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`.<br>`delete` is only available within objects containing tables. |

| | |
|---|---|
| `edit <table_name>` | Create or edit a table in the current object.<br>For example, in `config system admin`:<br>• edit the settings for the default `admin` administrator account by typing `edit admin`.<br>• add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`.<br>`edit` is an interactive sub-command: further sub-commands are available from within `edit`.<br>`edit` changes the prompt to reflect the table you are currently editing.<br>`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.<br>• In objects, `get` lists the table names (if present), or fields and their values.<br>• In a table, `get` lists the fields and their values. |
| `purge` | Remove all tables in the current object.<br>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.<br>`purge` is only available for objects containing tables.<br>**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 334`.<br>**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.<br>For example, in `config system admin`, you could rename `admin3` to `fwadmin` by typing `rename admin3 to fwadmin`.<br>`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.<br>  <br>Only administrators with super admin privileges may configure the feature on the primary HA unit while it is operating either in primary or config-primary mode.<br>To define HA attribute synchronization, configure the following:<br>`config <command>`<br>`chattr sync-disable ...`<br>`chattr sync-unset ...`<br>`end`<br>Use `chattr sync-disable` to disable any attributes from being synchronized across the HA cluster.<br>Use `chattr sync-unset` to reset the attribute's default synchronization behavior.<br>You can also enter `chattr` without an argument within a `config` command to display all attributes that can be configured for HA attribute synchronization.<br>Additionally, use the following `diagnose` commands:<br>• `diagnose system ha show-sync-diable-cfg`<br>Display all attributes that have been modified/disabled by the administrator.<br>• `diagnose system ha show-sync-diable-cfg all`<br>Display all attributes that are not synchronized, including both system default and settings disabled by the administrator.<br>• `diagnose system ha unset-sync-disable-cfg`<br>Change all modified/disabled attributes to the default synchronize action. Note that this command should be entered for both primary/config-primary and seconday/config-secondary units, as it may 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.<br>• In objects, `get` lists the table names (if present), or fields and their values.<br>• 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).<br>`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.<br>`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.<br>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`.<br>**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.<br>For example, in `config system admin`, after typing `edit admin`, typing `unset passwd` resets the password of the `admin` administrator account to the default (in this case, no password). |

**Example of field commands:**

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

```
set passwd my1stExamplePassword
```

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

# Permissions

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

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

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

- **System:** Can access areas regardless of whether an item pertains to the FortiMail unit itself or to a protected domain. The administrator's permissions are restricted only by his or her access profile.
- **A protected domain**: Can **only** access areas that are specifically assigned to that protected domain. The administrator **cannot** access system-wide settings, files or statistics, nor most settings that can affect other protected domains, regardless of whether access to those items would otherwise be allowed by his or her access profile. The administrator **cannot** access the CLI, nor the basic mode of the web UI (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 253.

There are three 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<br>• Can view and change all parts of the FortiMail unit's configuration, including uploading configuration backup files and restoring firmware default settings.<br>• Can release and delete quarantined email messages for all protected domains.<br>• Can back up and restore databases.<br>• Can manually update firmware and antivirus definitions.<br>• Can restart and shut down the FortiMail unit. | • Can create, view and change other administrator accounts with **Read & Write** and **Read Only** permissions in its own protected domain.<br>• Can only view and change settings, including profiles and policies, in its own protected domain.<br>• Can only view profiles and policies created by an administrator whose **Domain** is **system**.<br>• Can be only one per protected domain. |
| **Read & Write** | • Can only view and change its own administrator account.<br>• Can view and change parts of the FortiMail unit's configuration at the system and protected domain levels.<br>• Can release and delete quarantined email messages for all protected domains.<br>• Can back up and restore databases. | • Can only view and change its own administrator account.<br>• Can only view and change parts of the FortiMail unit's configuration in its own protected domain.<br>• Can only view profiles and policies created by an administrator whose **Domain** is **system.**<br>• Can release and delete quarantined email messages in its own protected domain. |
| **Read Only** | • Can only view and change its own administrator account.<br>• Can view the FortiMail unit configuration at the system and | • Can only view and change its own administrator account.<br>• Can only view settings in its own protected domain. |

| Permission | Domain: system | Domain: example.com |
|---|---|---|
| | protected domain levels<br>• Can release and delete quarantined email messages for all protected domains.<br>• Can back up databases. | • 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 web UI** | **In the CLI** | For each `config` command, there is an equivalent `get`/`show` command, unless otherwise noted.<br>`config` access requires write permission.<br>`get`/`show` access requires read permission. |
| **Policy** | `policy` | **Monitor > Mail Queue ...**<br>**Monitor > Greylist ...**<br>**Monitor > Reputation > Sender Reputation**<br>**Domain & User > Domain > Domain**<br>**System > Mail Setting > Proxies**<br>**Domain & User > User ...**<br>**Policy ...**<br>**Profile ...**<br>**AntiSpam > Greylist ...**<br>**AntiSpam > Bounce Verification > Settings**<br>**AntiSpam > Endpoint Reputation ...**<br>**AntiSpam > Bayesian ...** |
| | | `config antispam greylist exempt`<br>`config antispam bounce-verification key`<br>`config antispam settings`<br>`config antispam trusted ...`<br>`config domain`<br>`config mailsetting proxy-smtp`<br>`config policy ...`<br>`config profile ...`<br>`config user ...`<br>`diagnose ...`<br>`execute ...`<br>`config mailsetting relayserver` |
| **Block/Safelist** | `block-safe-list` | **Monitor > Endpoint Reputation > Auto blocklist**<br>**Maintenance > AntiSpam > Block/Safelist Maintenance**<br>**AntiSpam > Block/Safelist ...** |
| | | `N/A`<br>`diagnose ...`<br>`execute ...`<br>`get system status` |

| Access control area name | | Grants access to... |
|---|---|---|
| In the web UI | In the CLI | For each `config` command, there is an equivalent `get`/`show` command, unless otherwise noted.<br>`config` access requires write permission.<br>`get`/`show` access requires read permission. |
| | | `get system raid-performance`<br>`get system performance` |
| **Quarantine** | `quarantine` | **Monitor > Quarantine ...**<br>**AntiSpam > Quarantine > Quarantine Report**<br>**AntiSpam > Quarantine > System Quarantine Setting**<br>**AntiSpam > Quarantine > Control Account** |
| | | `diagnose ...`<br>`execute ...`<br>`config antispam quarantine-report`<br>`config mailsetting systemquarantine` |
| **Others** | `others` | **Monitor > System Status ...**<br>**Monitor > Archive > Email Archives**<br>**Monitor > Log ...**<br>**Monitor > Report ...**<br>**Maintenance** ... **except** the **Block/Safelist Maintenance** tab<br>**System** ...<br>**Mail Settings > Settings** ...<br>**Mail Settings > Address Book > Address Book**<br>**User > User Alias > User Alias**<br>**User > Address Map > Address Map**<br>**Email Archiving** ...<br>**Log and Report** ... |
| | | `config archive ...`<br>`config log ...`<br>`config mailsetting relayserver`<br>`config mailsetting storage`<br>`config report`<br>`config system ...`<br>`config user alias`<br>`config user map`<br>`diagnose ...`<br>`execute ...`<br>`get system status` |

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

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

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

# Tips and tricks

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

This section includes:



## Help

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

**Shortcuts and key commands:**

| Action | Keys |
|---|---|
| List valid word completions or subsequent words.<br>If multiple words could complete your entry, display all possible completions with helpful descriptions of each. | ? |
| Complete the word with the next available match.<br>Press the key multiple times to cycle through available matches. | Tab |

| Action | Keys |
|---|---|
| Recall the previous command.<br>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.<br>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.<br>For each line that you want to continue, terminate it with a backslash ( \ ).<br>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.

**Entering special characters:**

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

## Language support

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

For example, the host name must not contain special characters, and so the web UI 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 web UI or CLI. Using only ASCII, you do not need to worry about:

- mail transfer agent (MTA) encoding support
- mail user agent (MUA) language support

- web browser language support
- Telnet and/or SSH client support
- font availability
- compatibility of your input's encoding with the encoding/language setting of the web UI
- 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 web UI and your web browser or Telnet/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 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:**

Use `backup on page 334` to download the configuration file to a TFTP server, such as your management computer.

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

Use `restore config` on page 365 to upload the modified configuration file back to the FortiMail unit.

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

# config

`config` commands configure your FortiMail settings.

This chapter describes the following `config` commands:

mailsetting email-addr-handling on page 132
system geoip-override on page 286
system global on page 287
system ha on page 291
system interface on page 300
system link-monitor on page 305
system mailserver on page 306
system password-policy on page 312
system port-forwarding on page 313
system route on page 314
profile encryption on page 212 on page 197
profile content-action on page 203
profile dictionary on page 208
system saml on page 314
system scheduled-backup on page 315
system security crypto on page 315
system security authserver on page 316
system snmp community on page 316
system snmp sysinfo on page 317
system snmp threshold on page 318
system snmp user on page 319
system time manual on page 321
system fortiguard antispam on page 280
system fortisandbox on page 284
system time ntp on page 322
system webmail-language on page 326
system wccp settings on page 322
user alias on page 327
user map
user pki on page 330

# antispam adult-image-analysis

Use this command to configure the scanning behavior of FortiMail to detect adult images.

## Syntax

```
config antispam adult-image-analysis
   set max-size on page 41
   set min-size on page 41
   set rating-sensitivity on page 41
   set score-threshold on page 41
   set status {enable | disable} on page 41
end
```

| Variable | Description | Default |
|---|---|---|
| max-size | Set the maximum image size for the unit to analyze (KB). The valid range is 1-50000. | 500 |
| min-size | Set the minimum image size for the unit to analyze (KB). The valid range is 1-1000. | 10 |
| rating-sensitivity | Set the rating-sensitivity. The higher the number the higher the sensitivity. The valid range is 0-100. | 75 |
| score-threshold | Set the score threshold. The valid range is 1-9999. | 600 |
| status {enable \| disable} | Enable or disable adult image analysis. | enable |

# 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} on page 42
   set analysis-level{high | medium | low} on page 42
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 on page 43
antispam greylist exempt on page 45
antispam quarantine-report on page 47
antispam settings on page 48
antispam trusted on page 56

# antispam bounce-verification

Use this command to configure bounce address tagging and verification.

## Syntax

```
config antispam bounce-verification ...
   key on page 42
   tag-exempt-list on page 42
   verify-exempt-list on page 42
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 on page 43
antispam greylist exempt on page 45
antispam quarantine-report on page 47
antispam settings on page 48
antispam trusted on page 56

# antispam deepheader-analysis

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

Deepheader analysis examines the entire message header for spam characteristics.

Not all headers may be checked, depending on your configuration of antispam trusted on page 56.

## Syntax

```
config antispam deepheader-analysis
   set confidence <percent_float> on page 43
   set greyscale-level <level_int> on page 43
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.<br>The higher the calculated confidence value, the more likely the message is considered spam.<br>The deep header scan adds an `X-FEAS-DEEPHEADER:` line to the message header that includes the message's calculated confidence value. | 95.000000 |
| greyscale-level <level_int> | Type the grey scale threshold above which the deepheader scan will be skipped.<br>FortiGuard antispam service uses the grey scale of 1-9 to determine spam. 1-4 means the email is a spam for sure, while 9 is not a spam for sure.<br>Therefore, increasing this grey scale level will increase the probability to scan the email. This may increase spam catch rate but also increase false positives. | 7 |

## Related topics

profile antispam on page 169
antispam trusted on page 56
antispam greylist exempt on page 45
antispam settings on page 48

# antispam dmarc-report

Use this command to determine which, and how many, Domain-based Message Authentication, Reporting & Conformance (DMARC) author domains may receive DMARC reports. Administrators may use these reports to determine the effectiveness of their DMARC policies.

## Syntax

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

| Variable | Description | Default |
|---|---|---|
| status {enable \| disable \| monitor-only} | Enable to send DMARC reports to DMARC author domains of emails that went through DMARC check.<br>Set to `monitor-only` to collect DMARC data only. | disable |
| max-num-of-to-domain <integer> | Enter the maximum number of DMARC author domains you wish to send DMARC reports to per day.<br>Set the value between 1 to 300, with the maximum limit being FortiMail platform dependent:<br>• Up to VM02: 100<br>• VM02-VM04: 150<br>• VM04-VM08: 200<br>• VM08-VM16: 250<br>• VM16-End: 300 | 100 |
| from-addr-localpart <string> | Enter the local part of the sender email address you wish to send DMARC reports from. | noreply |

# 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> on page 45
end
```

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

## Related topics

profile antispam on page 169
antispam trusted on page 56

# 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> on page 45
end
```

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

## Related topics

antispam endpoint reputation blocklist on page 44

# 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> on page 46
      set recipient-pattern <recipient_pattern> on page 46
      set recipient-pattern-regexp {enable | disable} on page 46
```

```
      set reverse-dns-pattern <reverse-dns_pattern> on page 46
      set reverse-dns-pattern-regexp {enable | disable} on page 46
      set sender-ip <client_ipv4/mask> on page 46
      set sender-pattern <sender_pattern> on page 46
      set sender-pattern-regexp {enable | disable} on page 46
    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.<br>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.<br>Enter `disable` if you did **not** use regular expression syntax to define the pattern (that is, you entered a complete email address, or you entered a pattern using simple wild card characters * or ?). | disable |
| sender-ip <client_ ipv4/mask> | Enter the IP address and netmask of the SMTP client.<br>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.<br>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 on page 42

antispam deepheader-analysis on page 43

antispam quarantine-report on page 47

antispam settings on page 48

antispam trusted on page 56

# antispam quarantine-report

Use these commands to configure global settings for quarantine reports.

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

Alternatively, you can configure quarantine report settings specifically for each protected domain. For details, see config domain-setting on page 105.

## Syntax

```
config antispam quarantine-report
   set report-template-name {default | default-with-icons} on page 47
   set schedule-days <days_str> on page 47
   set schedule-hours <hour_int> on page 47
   set web-release-hostname <fortimail_fqdn> on page 47
   set web-release-https {enable | disable} on page 47
   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 <days_str> | Enter a space-delimited list of days of the week on which the FortiMail unit will generate spam reports. | (all days) |
| 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.<br>For example, to generate spam reports on 1:00 AM, 2:00 PM, and 11:00 PM, you would enter `1,14,23`.<br>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-https {enable \| disable} | Enable to redirect HTTP requests for FortiMail webmail and per-recipient quarantines to secure access using HTTPS.<br>**Note**: For this option to function properly, you must also enable both HTTP and HTTPS access protocols on the network interface to which the email user is connecting. | enable |
| web-release-unauth-expiry <hour_int> | Expiry time, in hours, of time limited webmail access to quarantine email without authorization. Set the value between 0 to 720. Set to 0 to disable (set by default). | 0 |

## Related topics

antispam bounce-verification on page 42

antispam deepheader-analysis on page 43

# antispam settings

Use these commands to configure global antispam settings.

## Syntax

```
config antispam settings
   set backend-verify <time_str> on page 49
   set bayesian-is-not-spam <local-part_str> on page 49
   set bayesian-is-spam <local-part_str> on page 49
   set bayesian-learn-is-not-spam <local-part_str> on page 49
   set bayesian-learn-is-spam <local-part_str> on page 49
   set bayesian-training-group <local-part_str> on page 49
   set blocklist-action {as-profile | discard | reject} on page 50
   set bounce-verification-action {as-profile | discard | reject} on page 50
   set bounce-verification-auto-delete-policy {never | one-month | one-year |
        six-months | three-months} on page 50
   set bounce-verification-status {enable | disable} on page 50
   set bounce-verification-tagexpiry <days_int> on page 50
   set carrier-endpoint-acct-response {enable | disable} on page 50
   set carrier-endpoint-acct-secret <password_str> on page 51
   set carrier-endpoint-acct-validate {enable | disable} on page 51
   set carrier-endpoint-attribute {Acct-Authentic ... Vendor-Specific) on page 51
   set carrier-endpoint-blocklist-window-size {15m | 30m | 60m | 90m | 120m |
        240m | 360m | 480m | 1440m} on page 51
   set carrier-endpoint-framed-ip-attr {Framed-IP-Address | Login-IP-Host |
        Login-IPv6-Host | NAS-IP-Address | NAS-IPv6-Address} on page 51
   set carrier-endpoint-framed-ip-order {host-order | network-order} on page 52
   set carrier-endpoint-radius-port <port_int> on page 52
   set carrier-endpoint-status {enable | disable} on page 52
   set delete-ctrl-account <local_part_str> on page 52
   set dmarc-failure-action {use-policy-action | use-profile-action | use-
        profile-action-with-none}
   set dynamic-safe-list-domain <domain_name_string> on page 52
   set dynamic-safe-list-state {enable | disable} on page 52
   set greylist-capacity <maximum_int> on page 52
   set greylist-check-level {disable | enable | low | high} on page 52
   set greylist-delay <1-120 minutes> on page 53
   set greylist-init-expiry-period <window_int> on page 53
   set greylist-ttl <ttl_int> on page 53
   set impersonation-analysis {manual | dynamic} on page 53
   set impersonation-analysis-level {aggressive | strict} on page 54
   set qr-code-image-max-size <integer>
   set qr-code-url-scan-status {enable | disable}
   set release-ctrl-account <local-part_str> on page 54
   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} on page 54
```

```
    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> on page 55
    set url-checking {strict | aggressive | extreme} on page 55
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.<br>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.<br>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.<br>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.<br>Unlike the `is-not-spam` email address, this email address will receive email that has **not** been previously seen by the Bayesian scanner.<br>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.<br>Unlike the `is-spam` email address, this email address will receive spam that has **not** been previously seen by the Bayesian scanner.<br>For example, if the local domain name of the FortiMail unit is example.com and you want to train the Bayesian database to recognize spam by sending control messages to learn-is-spam@example.com, you would enter `learn-is-spam`. | learn-is-spam |
| bayesian-training-group <local-part_str> | Enter the local-part portion of the email address that FortiMail administrators can use as their sender email address when forwarding email to the “learn is spam" email address or “learn is not spam" email address. Training messages sent from this sender email address will be used to train the global or per-domain Bayesian database (whichever is selected in the protected domain) but will **not** train any per-user Bayesian database. | default-grp |

| Variable | Description | Default |
|---|---|---|
| | 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. | |
| 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.<br>This setting affects email matching any system-wide, per-domain, per-session profile, or per-user blocklist.<br>For email messages involving a blocklisted email address, domain, or IP address, select one of the following options:<br>`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.<br>`discard`: Accept the message but delete and do not deliver it, without notifying the SMTP client.<br>`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.<br>`as-profile`: Perform the action selected in the antispam profile.<br>`discard`: Accept the message but then delete it without notifying the SMTP client.<br>`reject`: Reject the message, replying to the SMTP client with an SMTP rejection code. | as-profile |
| 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.<br>`never`: Never automatically delete an unused key.<br>`one-month`: Delete a key when it hasn't been used for 1 month.<br>`three-months`: Delete a key when it hasn't been used for 3 months.<br>`six-months`: Delete a key when it hasn't been used for 6 months.<br>`one-year`: Delete a key when it hasn't been used for 12 months.<br>The active key will not be automatically removed. | never |
| bounce-verification-status {enable \| disable} | Enable to activate bounce address tagging and verification.<br>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.<br>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 |

| Variable | Description | Default |
|---|---|---|
| carrier-endpoint-acct-secret <password_str> | Type the shared secret for RADIUS account response/request validation. | |
| carrier-endpoint-acct-validate {enable \| disable} | Enable/disable validating shared secret of account 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 network may use the “Calling-Station-ID” attribute while an ADSL network may use the “User-Name” attribute.<br>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.<br>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. | Calling-Station-Id (RADIUS attribute 31) |
| 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.<br>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.<br>By default, the endpoint user IP address uses the value of RADIUS attribute 8 (framed IP address).<br>However, if the endpoint IP address uses the value from different RADIUS attribute/number other than attribute 8, you can specify the corresponding attribute number with this command.<br>You can use the “diagnose debug application msisdn” command to capture RADIUS packets and find out what attribute name/number is used to hold the IP address value.<br>Note that you can specify multiple values, such as both IPv4 and IPv6 attributes. | Framed-IP-Address |

| Variable | Description | Default |
|---|---|---|
| carrier-endpoint-framed-ip-order {host-order \| network-order} | Select one of the following methods for endpoint IP address formatting:<br>**host-order**: format an IP address in host order, that is, the host portion is at the beginning. For example, 1.1.168.192.<br>**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.<br>This command starts the endpoint reputation daemon. You must start this daemon for the endpoint reputation feature to work. | enable |
| delete-ctrl-account <local_part_str> | Use this command to configure the email addresses through which email users can delete email from their per-recipient quarantines.<br>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.<br>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} | Set a DMARC failure action:<br>• `use-policy-action`: Respect all actions specified in the DMARC record.<br>• `use-profile-action`: Use the action specified in the antispam profile.<br>• `use-profile-action-with-none`: Respect p=none sender policy in the DMARC record, and use the antispam profile action otherwise. | use-profile-action-with-none |
| dynamic-safe-list-domain <domain_name_string> | 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.<br>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. | high |

| Variable | Description | Default |
|---|---|---|
| | Enable/disable greylist check, or set how aggressively to perform greylist check: high or low.<br>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 wil be greylisted. | |
| greylist-delay <1-120 minutes> | Enter the length in minutes of the greylist delay period.<br>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.<br>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.<br>The valid range is between 1 and 120 minutes. | 10 |
| greylist-init-expiry-period <window_int> | Enter the period of time in hours after the `greylistperiod`, during which pending greylist entries will be confirmed and converted into automatic greylist entries if the SMTP client retries delivery.<br>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.<br>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.<br>If the TTL elapses without an email message matching the automatic greylist entry, the entry expires and the greylist scanner removes the entry.<br>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.<br>To fight against email impersonation, you can map display names with email addresses and check email for the mapping.<br>You can choose whether the impersonation analysis uses the manual mapping entries or dynamic entries. You can also use both types of entries.<br>`manual`: Use the entries you manually entered under *Profile* > *AntiSpam* > *Impersonation*.<br>`dynamic`: Use the entries automatically learned by the FortiMail mail statistics service. To enable this service, enable `mailstat-service` under `config system global`. | manual |

| Variable | Description | Default |
|---|---|---|
| impersonation-analysis-level {aggressive \| strict} | `aggressive`: Choose this option to check the display name email domain part in Header From.<br>`strict`: Choose this option not to check the display name email domain.<br>For example, when you set an IA entry as:<br>`Display name: John Smith`<br>`Email address: john.smith@example.com`<br>While `example.com` is a protected domain.<br>Aggressive setting will block all of the following three senders:<br>• `"John Smith" <spammer@abc.com>`<br>• `"John.Smith@example.com" <spammer@abc.com>`<br>• `"OtherUser@example.com" <spammer@abc.com>`<br>But strict setting will only block the first two senders. | aggressive |
| qr-code-image-max-size <integer> | Enter the maximum QR code image size (in kilobytes) to scan. | 1000 |
| qr-code-url-scan-status {enable \| disable} | Enable or disable the scanning of QR code 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.<br>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.<br>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.<br>These statistics are tracked under **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.<br>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> | 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).<br>This command sets the time period. Other values are set under the `config profile session` command. | 30 |
| url-checking {strict \| aggressive \| extreme} | When you configure an antispam profile under *Profile* > *AntiSpam* > *AntiSpam*, if you enable FortiGuard scan and SURBL scan, FortiMail will scan for blocklisted URLs in email bodies.<br>There are two types of URLs:<br>• Absolute URLs strictly follow the URL syntax and include the URL scheme names, such as “http”, “https”, and “ftp”. For instance, http://www.example.com.<br>• Reference URLs do not contain the scheme names. For instance, example.com.<br>In some cases, you may want to scans for both absolute and reference URLs to improve the catch rate.<br>In some cases (for example, to lower false positive rates), you may want to scan for absolute URLs only.<br>`strict`: Choose this option to scan for absolute URLs only. Note that web sites without “http” or “https” but starting with “www” are also treated as absolute URLs. For instance, www.example.com.<br>`aggressive`: Choose this option to scan for both the absolute and reference URLs. Sender domains are also checked against FortiGuard.<br>`extreme`: Choose this option to scan for all URLs with or without schemes, including absolute URLs, reference URLs, URLs in text format, and sender domains. | strict |

## Related topics

antispam bounce-verification on page 42
antispam deepheader-analysis on page 43
antispam greylist exempt on page 45
antispam quarantine-report on page 47
antispam trusted on page 56

# 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> on page 56
end
```

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

## Related topics

antispam bounce-verification on page 42
antispam deepheader-analysis on page 43
antispam greylist exempt on page 45
antispam quarantine-report on page 47
antispam settings on page 48

# antispam url-fgas-exempt-list

Use this command to exempt URL list from FGAS rating

## Syntax

```
config antispam url-fgas-exempt-list
   edit <id>
      set url-exempt-pattern on page 57
      set pattern-type on page 57
end
```

| Variable | Description | Default |
|---|---|---|
| url-exempt-pattern | Enter the URLs that matches this pattern that are exempt from FGAS ratting. | |
| pattern-type | Enter the pattern type. | |

# 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> on page 57
      set destination {local | remote} on page 57
      set forward-address <recipient_email> on page 58
      set imap-access {enable | disable} on page 58
      set index-type {full | header |none} on page 58
      set local-quota <quota_int> on page 58
      set local-quota-cache <cache_int> on page 58
      set password <password_str> on page 58
      set quota-full {overwrite | noarchive} on page 58
      set remote-directory <path_str> on page 58
      set remote-ip <ftp_ipv4> on page 58
      set remote-password <password_Str> on page 58
      set remote-protocol {ftp | sftp} on page 58
      set remote-username <user_str> on page 58
      set retention-period <time_int>
      set rotation-hour <hour_int> on page 58
      set rotation-size <size_int> on page 58
      set rotation-time <time_int> on page 59
      set status {enable | disable} on page 59
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 |

| Variable | Description | Default |
|---|---|---|
| forward-address <recipient_email> | Enter the email address to which all archived messages will also be forwarded.<br>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).<br>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).<br>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:<br>`noarchive`: Discard the email message if the hard disk space is consumed and a new email message arrives.<br>`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. | |
| 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.<br>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> on page 59. | 0 |
| rotation-size <size_int> | Enter the maximum size of the current email archiving mailbox in megabytes (MB). | 200 |

| Variable | Description | Default |
|---|---|---|
| | 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).<br>The valid range is from 10 to 800 MB. | |
| rotation-time <time_int> | Enter the maximum age of the current email archiving mailbox in days.<br>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).<br>The valid range is from 1 to 365 days.<br>See rotation-hour <hour_int> on page 58 | 7 |
| status {enable \| disable} | Enable to activate email archiving. | enable |

## Related topics

archive exempt-policy on page 59

archive journal on page 60

# 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> on page 59
      set account <account_name> on page 59
      set pattern <string> on page 60
      set status {enable | disable} on page 60
      set type {sender | recipient | spam} on page 60
end
```

| Variable | Description | Default |
|---|---|---|
| <policy_id> | Enter the index number of the exemption policy.<br>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. | |

| Variable | Description | Default |
|---|---|---|
| pattern <string> | Enter a pattern, such as `user*@example.com`, that matches the attachment file name, text in the email body, text in the email subject, sender or recipient email addresses to which this exemption will apply. | * |
| status {enable \| disable} | Enable to activate the email archiving exemption. | enable |
| type {sender \| recipient \| spam} | Enter one of the following exemption match types:<br>`sender`: The sender email address will be evaluated for matches with `pattern`.<br>`recipient`: The recipient email address will be evaluated for matches with `pattern`.<br>`spam`: Do not archive spam emails. | sender |

## Related topics

archive journal on page 60

antispam url-fgas-exempt-list on page 56

# 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> on page 60
      set comments on page 60
      set email-archive-status {enable | disable}
      set host on page 60
      set recipient on page 60
      set scan-status {enable | disable}
      set sender on page 61
      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 |
| host | Enter the ip address or host name of the journal source. | |
| recipient | Enter the recipient email address. | |

| Variable | Description | Default |
|---|---|---|
| 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> on page 61
      set account <account_name> on page 61
      set pattern <string> on page 61
      set status {enable | disable} on page 61
      set type {attachment | body | deferral | recipient | sender | subject} on
           page 61
      set deferral-reason {spam-outbreak virus-outbreak sandbox}
end
```

| Variable | Description | Default |
|---|---|---|
| <policy_id> | Enter the index number of the policy.<br>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} | Enter one of the following match types:<br>• `attachment`: The attachment file name will be evaluated for matches with `pattern`.<br>• `body`: The body text will be evaluated for matches with `pattern`.<br>• `deferral`: The archive policy will be evaluated for matches with `deferral-reason`.<br>• `recipient`: The recipient email address will be evaluated for matches with `pattern`.<br>• `sender`: The sender email address will be evaluated for matches with | sender |

| Variable | Description | Default |
|---|---|---|
| | pattern.<br>• subject: The email subject will be evaluated for matches with pattern. | |
| deferral-reason {spam-outbreak virus-outbreak sandbox} | Note that this option is only available when type is set to deferral.<br>Enter one or more of the following reasons for deferring emails for analysis:<br>• fortisandbox: Defer email for sandbox scanning.<br>• spam-outbreak: Defer email for spam outbreak.<br>• virus-outbreak: Defer email for virus outbreak. | |

## Related topics

archive exempt-policy on page 59

antispam url-fgas-exempt-list on page 56

# 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 |

# customized-message

Use this command to configure replacement messages.

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

The FortiMail unit may also use replacement messages when notifying a recipient that it has blocked an email as spam or due to content filtering, or when sending a quarantine report.

You can customize the secure message notifications that secure email recipients receive when IBE encrypted email are sent to them, and configure simple network management protocol (SNMP) settings.

## Syntax

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

```
config customized-message
   edit <message_name> on page 63
   next
end
```

| Variable | Description | Default |
|---|---|---|
| <message_name> | Select the replacement message that you want to customize.<br>The message names include:<br>alert-email on page 64<br>as-sender-rate-notify on page 65<br>attachment-filtering-notify<br>content-disarm-reconstruct<br>custom-webmail-login on page 68<br>disclaimer-insertion<br>email-template-av-repack on page 69<br>email-template-notify-generic on page 70<br>ibe-login-page<br>ibe-notify-account-delete<br>ibe-notify-account-expiry<br>ibe-notify-account-expiry-alert<br>ibe-notify-account-lock<br>ibe-notify-account-reset on page 74<br>ibe-notify-account-reset-done on page 75<br>ibe-notify-activation<br>customized-message<br>ibe-notify-password-reset on page 77<br>ibe-notify-password-reset-done<br>ibe-notify-pull-message on page 78<br>ibe-notify-push-message on page 79<br>ibe-notify-user-register-done on page 80<br>ibe-notify-wread-notif on page 81<br>ibe-notify-wunread-rcpt on page 81<br>ibe-notify-wunread-sender on page 82<br>ibe-password-reset-page<br>ibe-register-page<br>ibe-tfa-email-verify<br>ibe-tfa-register-page<br>ibe-tfa-sms-verify<br>log-report on page 86 | |

| Variable | Description | Default |
|---|---|---|
| | login-disclaimer on page 87<br>reject-content-attachment on page 88<br>reject-content-message on page 88<br>reject-delivery on page 89<br>reject-endpoint-reputation on page 89<br>reject-spam on page 90<br>reject-virus-message on page 91<br>reject-virus-suspicious on page 91<br>replace-content-attachment on page 92<br>replace-content-body on page 93<br>replace-content-subject on page 93<br>replace-dlp-body<br>replace-dlp-subject<br>replace-virus-message on page 95<br>replace-virus-suspicious on page 96<br>report-active-mailbox-summary<br>report-quarantine-summary on page 97<br>uri-protection-allow-with-confirmation<br>uri-protection-block<br>uri-protection-remove<br>uri-protection-uri-evaluation | |

## Related topics

config domain-setting on page 105

config policy recipient on page 115

## alert-email

Use this sub-command to configure the variables and the default email template of the alert email.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit alert-email
   config variable
      edit <name> on page 65
         set content on page 65
         set display-name on page 65
   config email-template
      edit default
         set from <string> on page 65
```

```
        set html-body <string> on page 65
        set subject <string> on page 65
        set text-body <string> on page 65
end
```

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

## as-sender-rate-notify

Use this sub-command to configure the variables and the default email template of the notifications for spam sender's sending rate.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit as-sender-rate-notify
   config variable
      edit <name> on page 65
         set content on page 65
         set display-name on page 66
   config email-template
      edit default
         set env-from <string> on page 66
         set from <string> on page 66
         set html-body <string> on page 66
         set subject <string> on page 66
         set text-body <string> on page 66
         set to <string> on page 66
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%MEETING%%. | |
| content | Enter the content for the variable. | |

| Variable | Description | Default |
|---|---|---|
| display-name | Enter the display name for the variable. For example, the display name for %%MEETING%% can be weekly meeting. | |
| env-from <string> | Enter the replacement message for the email Envelope From field. | |
| from <string> | Enter the replacement message for the email From field. | |
| html-body <string> | Enter the replacement email body in HTML format. | |
| subject <string> | Enter the replacement message for the email Subject header. | |
| text-body <string> | Enter the replacement email body in text format. | |
| to <string> | Enter the replacement message for the email To field. | |

## attachment-filtering-notify

Use this sub-command to configure the variables and the default email template of the notification for attachment filtering.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit attachment-filtering-notify
   config variable
      edit <name>
         set content
         set display-name
   config email-template
      edit default
         set env-from
         set env-to
         set from <string>
         set html-body <string>
         set subject <string>
         set text-body <string>
         set to <string>
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%MEETING%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%MEETING%% can be weeklymeeting. | |
| env-from | Enter the replacement message for the email Envelope From field. | |

| Variable | Description | Default |
|---|---|---|
| <string> | | |
| env-to <string> | Enter the replacement message for the email Envelope To field. | |
| from <string> | Enter the replacement message for the email From field. | |
| html-body <string> | Enter the replacement email body in HTML format. | |
| subject <string> | Enter the replacement message for the email Subject header. | |
| text-body <string> | Enter the replacement email body in text format. | |
| to <string> | Enter the replacement message for the email To field. | |

## content-disarm-reconstruct

Use this sub-command to configure the variables and the default content of the notification message for Office and/or PDF attachment content disarm and reconstruction (CDR).

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit content-disarm-reconstruct
   config variable
      edit <name>
         set content
         set display-name
   config message
      edit default
         set content <string>
         set format {html | multiline | text}
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as `%%FILE%%`. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for `%%FILE%%` can be `Login`. | |
| content <string> | Enter the replacement message for the webmail login. | |
| format {html \| multiline \| text} | Select the format for the webmail login. | html |

## custom-webmail-login

Use this sub-command to configure the variables and the default content of the webmail login.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit custom-webmail-login
   config variable
      edit <name> on page 67
         set content on page 67
         set display-name on page 67
   config message
      edit default
         set content <string> on page 67
         set format {html | multiline | text} on page 67
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%FILE%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%FILE%% can be Login. | |
| content <string> | Enter the replacement message for the webmail login. | |
| format {html \| multiline \| text} | Select the format for the webmail login. | html |

## disclaimer-insertion

Use this sub-command to configure the variables and the default content of the disclaimer insertion message.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit disclaimer-insertion
   config variable
      edit <name>
         set content
         set display-name
   config message
      edit default
         set content <string>
         set format {html | multiline | text}
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%FILE%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%FILE%% can be Login. | |
| content <string> | Enter the replacement message for the webmail login. | |
| format {html \| multiline \| text} | Select the format for the webmail login. | html |

## email-template-av-repack

Use this sub-command to configure the variables and the default content of the email template for antivirus action.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit email-template-av-repack
   config variable
      edit <name> on page 69
         set content on page 69
         set display-name on page 69
   config email-template
      edit default
         set from <string> on page 69
         set html-body <string> on page 69
         set subject <string> on page 69
         set text-body <string> on page 69
end
```

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

## email-template-notify-generic

Use this sub-command to configure the variables and the default content of the email template for generic notifications.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit email-template-notify-generic
   config variable
      edit <name> on page 70
         set content on page 70
         set display-name on page 70
   config email-template
      edit default
         set env-from <string> on page 70
         set from <string> on page 70
         set html-body <string> on page 70
         set subject <string> on page 70
         set text-body <string> on page 70
         set to <string> on page 70
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%FILE%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%FILE%% can be Template. | |
| env-from <string> | Enter the replacement message for the email Envelope From field. | |
| from <string> | Enter the replacement message for the email From field. | |
| html-body <string> | Enter the replacement email body in HTML format. | |
| subject <string> | Enter the replacement message for the email Subject header. | |
| text-body <string> | Enter the replacement email body in text format. | |
| to <string> | Enter the replacement message for the email To field. | |

## ibe-login-page

Use this sub-command to configure the variables and the default replacement message for the custom IBE login page.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-login-page
   config variable
      edit <name>
         set content
         set display-name
   config message
      edit default
         set content <string>
         set format {html | multiline | text}
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%WARNING%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%WARNING%% can be Notice. | |
| content <string> | Enter the replacement message for suspicious email attachments. | |
| format {html \| multiline \| text} | Select the format for the replacement message of suspicious email attachments. | text |

## ibe-notify-account-delete

Use this sub-command to configure the variables and the default email template of the IBE account delete notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-account-delete
   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 notification. | |

| Variable | Description | Default |
|---|---|---|
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the `subject` field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-account-expiry

Use this sub-command to configure the variables and the default email template of the IBE account expiry notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-account-expiry
   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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the `subject` field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-account-expiry-alert

Use this sub-command to configure the variables and the default email template of the IBE account expiry alert notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-account-expiry-alert
   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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-account-lock

Use this sub-command to configure the variables and the default email template of the IBE account lock notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-account-lock
   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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-account-reset

Use this sub-command to configure the variables and the default email template of the IBE account reset notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-account-reset
   config variable
      edit <name> on page 71
         set content on page 71
         set display-name on page 71
   config email-template
      edit default
         set from <string> on page 71
         set html-body <string> on page 72
         set subject <string> on page 72
         set text-body <string> on page 72
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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-account-reset-done

Use this sub-command to configure the variables and the default email template of the IBE account reset completion notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-account-reset-done
   config variable
      edit <name> on page 75
         set content on page 75
         set display-name on page 75
   config email-template
      edit default
         set from <string> on page 75
         set global-bayesian {enable | disable} on page 107
         set subject <string> on page 75
         set text-body <string> on page 75
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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-activation

Use this sub-command to configure the variables and the default email template for the account activation notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-activation
   config variable
      edit <name>
         set content
         set display-name
   config email-template
```

```
        edit default
           set env-from <string>
           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. | |
| env-from <string> | Enter the replacement message for the Envelope From field of the notification. | |
| from <string> | Enter the replacement message for the From field of the notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-config-change

Use this sub-command to configure the variables and the default email template of the IBE account security settings changed notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-config-change
   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%%. | |

| Variable | Description | Default |
|---|---|---|
| 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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the `subject` field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-password-reset

Use this sub-command to configure the variables and the default email template of the IBE password reset notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-password-reset
   config variable
      edit <name> on page 77
         set content on page 77
         set display-name on page 77
   config email-template
      edit default
         set from <string> on page 77
         set html-body <string> on page 77
         set subject <string> on page 77
         set text-body <string> on page 77
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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the `subject` field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-password-reset-done

Use this sub-command to configure the variables and the default email template of the IBE password reset completion notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-password-reset-done
   config variable
      edit <name> on page 78
         set content on page 78
         set display-name on page 78
   config email-template
      edit default
         set from <string> on page 78
         set html-body <string> on page 78
         set subject <string> on page 78
         set text-body <string> on page 78
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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-pull-message

Use this sub-command to configure the variables and the default email template of the secure message notification containing a link which the Webmail users can click to read the message.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-pull-message
   config variable
      edit <name> on page 79
         set content on page 79
         set display-name on page 79
```

```
    config email-template
       edit default
          set from <string> on page 79
          set html-body <string> on page 79
          set subject <string> on page 79
          set text-body <string> on page 79
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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-push-message

Use this sub-command to configure the variables and the default email template of the secure message notification with an attachment containing the secure message.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-push-message
   config variable
      edit <name> on page 79
         set content on page 79
         set display-name on page 80
   config email-template
      edit default
         set from <string> on page 80
         set html-body <string> on page 80
         set subject <string> on page 80
         set text-body <string> on page 80
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. | |

| Variable | Description | Default |
|---|---|---|
| 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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-user-register-done

Use this sub-command to configure the variables and the default email template of the IBE user registration notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-user-register-done
   config variable
      edit <name> on page 80
         set content on page 80
         set display-name on page 80
   config email-template
      edit default
         set from <string> on page 80
         set html-body <string> on page 80
         set subject <string> on page 80
         set text-body <string> on page 80
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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-wread-notif

Use this sub-command to configure the variables and the default email template of the IBE “read” notification which is the first time the message is read.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-wread-notif
   config variable
      edit <name> on page 81
         set content on page 81
         set display-name on page 81
   config email-template
      edit default
         set from <string> on page 81
         set html-body <string> on page 81
         set subject <string> on page 81
         set text-body <string> on page 81
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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-wunread-rcpt

Use this sub-command to configure the variables and the default email template of the IBE “unread” notification to the recipient when a mail remains unread for a period of time.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-wunread-rcpt
   config variable
      edit <name> on page 82
         set content on page 82
         set display-name on page 82
```

```
    config email-template
       edit default
          set from <string> on page 82
          set html-body <string> on page 82
          set subject <string> on page 82
          set text-body <string> on page 82
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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-notify-wunread-sender

Use this sub-command to configure the variables and the default email template of the IBE “unread” notification to the sender when a mail remains unread for a period of time.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-notify-wread-notif
   config variable
      edit <name> on page 82
         set content on page 82
         set display-name on page 83
   config email-template
      edit default
         set from <string> on page 83
         set html-body <string> on page 83
         set subject <string> on page 83
         set text-body <string> on page 83
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. | |

| Variable | Description | Default |
|---|---|---|
| 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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the `subject` field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-password-reset-page

Use this sub-command to configure the variables and the default content of the custom IBE password reset page.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-password-reset-page
   config variable
      edit <name>
         set content
         set display-name
   config message
      edit default
         set content <string>
         set format {html | multiline | text}
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as `%%FILE%%`. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for `%%FILE%%` can be `Login`. | |
| content <string> | Enter the replacement message for the webmail login. | |
| format {html \| multiline \| text} | Select the format for the webmail login. | text |

## ibe-register-page

Use this sub-command to configure the variables and the default content of the custom IBE user registration page.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-register-page
   config variable
      edit <name>
         set content
         set display-name
   config message
      edit default
         set content <string>
         set format {html | multiline | text}
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%FILE%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%FILE%% can be Login. | |
| content <string> | Enter the replacement message for the webmail login. | |
| format {html \| multiline \| text} | Select the format for the webmail login. | text |

## ibe-tfa-email-verify

Use this sub-command to configure the variables and the default email template for the secure token notification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-tfa-email-verify
   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. | |

| Variable | Description | Default |
|---|---|---|
| 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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## ibe-tfa-register-page

Use this sub-command to configure the variables and the default content of the custom IBE user two-factor authentication registration page.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-tfa-register-page
   config variable
      edit <name>
         set content
         set display-name
   config message
      edit default
         set content <string>
         set format {html | multiline | text}
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%FILE%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%FILE%% can be Login. | |
| content <string> | Enter the replacement message for the webmail login. | |
| format {html \| multiline \| text} | Select the format for the webmail login. | text |

## ibe-tfa-sms-verify

Use this sub-command to configure the variables and the default content of the custom IBE user two-factor authentication SMS verification.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit ibe-tfa-sms-verify
   config variable
      edit <name>
         set content
         set display-name
   config message
      edit default
         set content <string>
         set format {html | multiline | text}
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%FILE%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%FILE%% can be Login. | |
| content <string> | Enter the replacement message for the webmail login. | |
| format {html \| multiline \| text} | Select the format for the webmail login. | text |

## log-report

Use this sub-command to configure the variables and the default content of the FortiMail log report.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit log-report
   config variable
      edit <name> on page 86
         set content on page 87
         set display-name on page 87
   config message
      edit default
         set env-from <string> on page 87
         set from <string> on page 87
         set html-body <string> on page 87
         set subject <string> on page 87
         set text-body <string> on page 87
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%WARNING%%. | |

| Variable | Description | Default |
|---|---|---|
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for `%%WARNING%%` can be `Disclaimer`. | |
| env-from <string> | Enter the replacement message for the email Envelope From field. | |
| from <string> | Enter the replacement message for the email From field. | |
| html-body <string> | Enter the replacement email body in HTML format. | |
| subject <string> | Enter the replacement message for the email Subject header. | |
| text-body <string> | Enter the replacement email body in text format. | |

## login-disclaimer

Use this sub-command to configure the variables and the default content of the FortiMail system login disclaimer.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit login-disclaimer
   config variable
      edit <name> on page 87
         set content on page 87
         set display-name on page 87
   config message
      edit default
         set content <string> on page 87
         set format {html | multiline | text} on page 87
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as `%%WARNING%%`. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for `%%WARNING%%` can be `Disclaimer`. | |
| content <string> | Enter the replacement message for the login disclaimer. | |
| format {html \| multiline \| text} | Select the format for the login disclaimer. | html |

## reject-content-attachment

Use this sub-command to configure the variables and the default content of the attachment filtering message. This message is sent when an email is rejected for containing banned attachments.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit reject-content-attachment
   config variable
      edit <name> on page 88
         set content on page 88
         set display-name on page 88
   config message
      edit default
         set content <string> on page 88
         set format {html | multiline | text} on page 88
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%REJECTION%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice. | |
| content <string> | Enter the replacement message for the attachment filtering message. | |
| format {html \| multiline \| text} | Select the format for the attachment filtering message. | html |

## reject-content-message

Use this sub-command to configure the variables and the default content of the content filtering message. This message is sent when an email is rejected for containing sensitive content.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit reject-content-message
   config variable
      edit <name> on page 89
         set content on page 89
         set display-name on page 89
   config message
      edit default
         set content <string> on page 89
         set format {html | multiline | text} on page 89
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%REJECTION%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice. | |
| content <string> | Enter the replacement message for the content filtering message. | |
| format {html \| multiline \| text} | Select the format for the content filtering message. | html |

## reject-delivery

Use this sub-command to configure the variables and the default content of the message delivery failure message.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit reject-delivery
   config variable
      edit <name> on page 89
         set content on page 89
         set display-name on page 89
   config message
      edit default
         set content <string> on page 89
         set format {html | multiline | text} on page 89
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%REJECTION%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice. | |
| content <string> | Enter the replacement message for the delivery failure message. | |
| format {html \| multiline \| text} | Select the format for the delivery failure message. | html |

## reject-endpoint-reputation

Use this sub-command to configure the variables and the default content of the content filtering message. This message is sent when an email is rejected for carrier endpoint reputation check.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit reject-endpoint-reputation
   config variable
      edit <name> on page 89
         set content on page 89
         set display-name on page 89
   config message
      edit default
         set content <string> on page 89
         set format {html | multiline | text} on page 89
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%REJECTION%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Endpoint. | |
| content <string> | Enter the replacement message for the content filtering message. | |
| format {html \| multiline \| text} | Select the format for the content filtering message. | html |

## reject-spam

Use this sub-command to configure the variables and the default content of the spam message. This message is sent when an email is rejected for being detected as spam.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit reject-spam
   config variable
      edit <name> on page 90
         set content on page 90
         set display-name on page 91
   config message
      edit default
         set content <string> on page 91
         set format {html | multiline | text} on page 91
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%REJECTION%%. | |
| content | Enter the content for the variable. | |

| Variable | Description | Default |
|---|---|---|
| display-name | Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice. | |
| content <string> | Enter the replacement message for the spam message. | |
| format {html \| multiline \| text} | Select the format for the spam message. | html |

## reject-virus-message

Use this sub-command to configure the variables and the default content of the virus message. This message is sent when an email is rejected for being infected with virus.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit reject-virus-message
   config variable
      edit <name> on page 91
         set content on page 91
         set display-name on page 91
   config message
      edit default
         set content <string> on page 91
         set format {html | multiline | text} on page 91
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%REJECTION%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice. | |
| content <string> | Enter the replacement message for the virus message. | |
| format {html \| multiline \| text} | Select the format for the virus message. | html |

## reject-virus-suspicious

Use this sub-command to configure the variables and the default content of the suspicious message. This message is sent when an email is rejected for containing suspicious components.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit reject-virus-suspicious
   config variable
      edit <name> on page 92
         set content on page 92
         set display-name on page 92
   config message
      edit default
         set content <string> on page 92
         set format {html | multiline | text} on page 92
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%REJECTION%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%REJECTION%% can be Notice. | |
| content <string> | Enter the replacement message for the suspicious message. | |
| format {html \| multiline \| text} | Select the format for the suspicious message. | html |

## replace-content-attachment

Use this sub-command to create the variables for and replace the default content of the attachment filtering message. This message is sent when the attachment of an email is blocked.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit replace-content-attachment
   config variable
      edit <name> on page 92
         set content on page 92
         set display-name on page 92
   config message
      edit default
         set content <string> on page 92
         set format {html | multiline | text} on page 93
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%BLOCK%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%BLOCK%% can be Notice. | |
| content <string> | Enter the replacement message for the attachment filtering message. | |

| Variable | Description | Default |
|---|---|---|
| format {html \| multiline \| text} | Select the format for the attachment filtering message. | html |

## replace-content-body

Use this sub-command to create the variables for and replace the default body of the content filtering message. This message is sent when an email is rejected for containing corporate sensitive data.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit replace-content-body
   config variable
      edit <name> on page 93
         set content on page 93
         set display-name on page 93
   config message
      edit default
         set content <string> on page 93
         set format {html | multiline | text} on page 93
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%REJECT%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%REJECT%% can be Notice. | |
| content <string> | Enter the replacement message for the body of the content filtering message. | |
| format {html \| multiline \| text} | Select the format for the body of the content filtering message. | html |

## replace-content-subject

Use this sub-command to create the variables for and replace the default subject of the content filtering message. This message is sent when an email is rejected for containing corporate sensitive data.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit replace-content-subject
   config variable
      edit <name> on page 94
         set content on page 94
         set display-name on page 94
```

```
    config message
       edit default
          set content <string> on page 94
          set format {html | multiline | text} on page 94
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%REJECT%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%REJECT%% can be Notice. | |
| content <string> | Enter the replacement message for the subject of the content filtering message. | |
| format {html \| multiline \| text} | Select the format for the subject of content filtering message. | html |

## replace-dlp-body

Use this sub-command to configure the variables and the default replacement message body for email data loss prevention.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit replace-dlp-body
   config variable
      edit <name> on page 94
         set content on page 94
         set display-name on page 94
   config message
      edit default
         set content <string> on page 94
         set format {html | multiline | text} on page 94
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%WARNING%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%WARNING%% can be Notice. | |
| content <string> | Enter the replacement message for infected email attachments. | |
| format {html \| multiline \| text} | Select the format for the replacement message of infected email attachments. | multiline |

## replace-dlp-subject

Use this sub-command to configure the variables and the default replacement message subject for email data loss prevention.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit replace-dlp-subject
   config variable
      edit <name> on page 94
         set content on page 94
         set display-name on page 94
   config message
      edit default
         set content <string> on page 94
         set format {html | multiline | text} on page 94
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%WARNING%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%WARNING%% can be Notice. | |
| content <string> | Enter the replacement message for infected email attachments. | |
| format {html \| multiline \| text} | Select the format for the replacement message of infected email attachments. | multiline |

## replace-virus-message

Use this sub-command to configure the variables and the default replacement message for infected email attachments. This message is sent when an email's attachment is removed for being infected with a virus.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit replace-virus-message
   config variable
      edit <name> on page 94
         set content on page 94
         set display-name on page 94
   config message
      edit default
         set content <string> on page 94
         set format {html | multiline | text} on page 94
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%WARNING%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%WARNING%% can be Notice. | |
| content <string> | Enter the replacement message for infected email attachments. | |
| format {html \| multiline \| text} | Select the format for the replacement message of infected email attachments. | html |

## replace-virus-suspicious

Use this sub-command to configure the variables and the default replacement message for suspicious email attachments. This message is sent when an email's attachment is removed for containing suspicious components.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit replace-virus-suspicious
   config variable
      edit <name> on page 71
         set content on page 71
         set display-name on page 71
   config message
      edit default
         set content <string> on page 71
         set format {html | multiline | text} on page 71
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%WARNING%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%WARNING%% can be Notice. | |
| content <string> | Enter the replacement message for suspicious email attachments. | |
| format {html \| multiline \| text} | Select the format for the replacement message of suspicious email attachments. | html |

## report-active-mailbox-summary

Use this sub-command to configure the variables and the default email template of the mailbox statistic report.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit report-active-mailbox-summary
   config variable
      edit <name>
         set content
         set display-name
   config email-template
      edit default
         set env-from <string>
         ste 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 notification. | |
| html-body <string> | Enter the replacement message for the notification email body in HTML code. | |
| subject <string> | Enter the replacement message for the subject field of the notification. | |
| text-body <string> | Enter the replacement message for the notification email body in text format. | |

## report-quarantine-summary

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

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit report-quarantine-summary
   config variable
      edit <name> on page 98
         set content on page 98
         set display-name on page 98
   config email-template
      edit default
         set from <string> on page 98
         set html-body <string> on page 80
         set subject <string> on page 80
```

```
        set text-body <string> on page 80
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. | |

## uri-protection-allow-with-confirmation

Use this sub-command to configure the variables and the default replacement message for allowing suspicious URIs with user confirmation.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit uri-protection-allow-with-confirmation
   config variable
      edit <name>
         set content
         set display-name
   config message
      edit default
         set content <string>
         set format {html | multiline | text}
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%WARNING%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%WARNING%% can be Notice. | |
| content <string> | Enter the replacement message for suspicious email attachments. | |
| format {html \| multiline \| text} | Select the format for the replacement message of suspicious email attachments. | text |

## uri-protection-block

Use this sub-command to configure the variables and the default replacement message for blocking suspicious URIs.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit uri-protection-block
   config variable
      edit <name>
         set content
         set display-name
   config message
      edit default
         set content <string>
         set format {html | multiline | text}
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as `%%WARNING%%`. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for `%%WARNING%%` can be `Notice`. | |
| content <string> | Enter the replacement message for suspicious email attachments. | |
| format {html \| multiline \| text} | Select the format for the replacement message of suspicious email attachments. | text |

## uri-protection-remove

Use this sub-command to configure the variables and the default replacement message for removed URIs.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit uri-protection-remove
   config variable
      edit <name>
         set content
         set display-name
   config message
      edit default
         set content <string>
         set format {html | multiline | text}
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%WARNING%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%WARNING%% can be Notice. | |
| content <string> | Enter the replacement message for suspicious email attachments. | |
| format {html \| multiline \| text} | Select the format for the replacement message of suspicious email attachments. | text |

## uri-protection-uri-evaluation

Use this sub-command to configure the variables and the default replacement message for click protection URI evaluation.

### Syntax

This sub-command is available from within the command customized-message on page 62.

```
edit uri-protection-uri-evaluation
   config variable
      edit <name>
         set content
         set display-name
   config message
      edit default
         set content <string>
         set format {html | multiline | text}
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter a variable name that you want to add or edit, such as %%WARNING%%. | |
| content | Enter the content for the variable. | |
| display-name | Enter the display name for the variable. For example, the display name for %%WARNING%% can be Notice. | |
| content <string> | Enter the replacement message for suspicious email attachments. | |
| format {html \| multiline \| text} | Select the format for the replacement message of suspicious email attachments. | text |

# dlp scan-rules

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

## Syntax

```
config dlp scan-rules
   edit <rule_name> on page 101
        config conditions on page 101
           edit <condition_id>
              set attribute {attachment | attachment_metadata | body | body_and_
                   attachment | header | recipient | sender | sender_or_recipient
                   | subject} on page 101
              set file-pattern {archive | audio | encrypted | executable_windows |
                   image | msoffice | openoffice | script | video} on page 102
              set group-type {local | ldap} on page 102
              set ldap-profile <profile_name> on page 102
              set operator {contain | contain_file_pattern | contain_sensitive_data
                   | empty | equal | external | internal | match | not_contain |
                   not_equal | not_present | password_protected | present} on page
                   102
              set sensitive-data {...} on page 102
              set value <string> on page 102
        config exceptions on page 101
           edit <exception_id>
              set attribute {attachment | attachment_metadata | body | body_and_
                   attachment | header | recipient | sender | sender_or_recipient
                   | subject} on page 101
              set file-pattern {archive | audio | encrypted | executable_windows |
                   image | msoffice | openoffice | script | video} on page 102
              set group-type {local | ldap} on page 102
              set ldap-profile <profile_name> on page 102
              set operator {contain | contain_file_pattern | contain_sensitive_data
                   | empty | equal | external | internal | match | not_contain |
                   not_equal | not_present | password_protected | present} on page
                   102
              set sensitive-data {...} on page 102
              set value <string> on page 102
      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. | |
| 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 |

| Variable | Description | Default |
|---|---|---|
| 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> on page 103
    config config cal resource...
    config config customized-message on page 103...
    config config domain-info...
    config config domain-setting on page 105...
    config file filter...
    config config policy recipient on page 115...
    config config profile account-sync...
    config profile antispam on page 169...
    config profile antispam-action on page 181...
    config profile antivirus on page 185...
    config profile antivirus-action on page 187...
    config profile authentication on page 191...
    config profile content on page 197...
    config profile content-action on page 203...
    config profile cousin-domain...
    config profile email-address-group ...
    config profile impersonation on page 213...
    config profile notification...
    config profile resource on page 233...
    config config user mail on page 120...
  next
```

```
   end
```

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

## config 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 <string> | Enter a description for the calendar resource entry. | |
| display-name <string> | 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 |

## config 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> on page 104
            set content on page 104
            set display-name on page 104
      config email-template
         edit default
            set from <string> on page 104
            set html-body <string> on page 104
            set subject <string> on page 104
            set text-body <string> on page 104
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. | |

## config 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. | |

# config domain-setting

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

## Syntax

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

```
config domain-setting
   config sender-addr-rate-ctrl-exempt
      edit <id>
         set sender-pattern <string>
         set pattern-type {default | regexp}
   end
   set addressbook {domain | none | system} on page 106
   set bypass-bounce-verification {enable | disable} on page 106
   set disclaimer-incoming-body-content
   set disclaimer-incoming-body-content-html
   set disclaimer-incoming-body-location
   set disclaimer-incoming-body-status {enable | disable}
   set disclaimer-incoming-header-insertion-name
   set disclaimer-incoming-header-insertion-value
   set disclaimer-incoming-header-status {enable | disable}
   set disclaimer-outgoing-body-content
   set disclaimer-outgoing-body-content-html
   set disclaimer-outgoing-body-location
   set disclaimer-outgoing-body-status {enable | disable}
   set disclaimer-outgoing-header-insertion-name
   set disclaimer-outgoing-header-insertion-value
   set disclaimer-outgoing-header-status {enable | disable}
   set dmarc-report-status {disable | enable | monitor-only | use-system-setting}
   set email-continuity-status {enable | disable}
   set fallback-host {<smtp-server_fqdn> | <smtp-server_ipv4>} on page 106
   set fallback-port <port_int> on page 106
   set fallback-use-smtps {enable | disable} on page 107
   set global-bayesian {enable | disable} on page 107
   set greeting-with-host-name {domainname | hostname | othername} on page 107
   set host <host_name> on page 107
   set ip-pool <pool_name> on page 107
   set ip-pool-direction {outgoing | incoming | both} on page 108
   set is-service-domain {enable | disable}
   set is-sub-domain {enable | disable} on page 108
   set ldap-asav-profile <ldap-profile_name> on page 108
   set ldap-asav-status {enable | disable} on page 108
   set ldap-domain-routing-port <port_int> on page 108
   set ldap-domain-routing-profile <ldap-profile_name> on page 109
   set ldap-domain-routing-smtps {enable |disable} on page 109
   set ldap-groupowner-profile <ldap-profile_name> on page 109
   set ldap-routing-profile <ldap-profile_name> on page 109
   set ldap-routing-status {enable | disable} on page 109
   set ldap-user-profile <profile_name> on page 109
   set max-message-size <limit_int> on page 109
   set other-helo-greeting <string> on page 109
   set port <smtp-port_int> on page 109
   set quarantine-report-schedule-status {enable | disable} on page 109
   set quarantine-report-status {enable | disable} on page 109
```

```
    set quarantine-report-to-alt {enable | disable} on page 110
    set quarantine-report-to-alt-addr <recipient_email> on page 110
    set quarantine-report-to-individual {enable | disable} on page 110
    set quarantine-report-to-ldap-groupowner {enable | disable} on page 110
    set recipient-verification {disable | ldap | smtp} on page 110
    set recipient-verification-background {disable | ldap | smtp} on page 111
    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} on page 112
    set remove-outgoing-received-header {enable | disable} on page 112
    set sender-addr-rate-ctrl-action
    set sender-addr-rate-ctrl-max-msgs <integer> on page 113
    set sender-addr-rate-ctrl-max-msgs-state {enable | disable} on page 113
    set sender-addr-rate-ctrl-max-recipients
    set sender-addr-rate-ctrl-max-recipients-state {enable | disable}
    set sender-addr-rate-ctrl-max-size <integer> on page 113
    set sender-addr-rate-ctrl-max-size-state {enable | disable} on page 113
    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} on page 113
    set sender-addr-rate-notification-state {enable | disable}
    set smtp-recipient-verification-command {rcpt | vrfy} on page 113
    set smtp-recipient-verification-accept-reply-string <accept_string> on page
      113
    set tp-hidden {no | yes} on page 113
    set tp-server-on-port <port_int> on page 114
    set tp-use-domain-mta {yes | no} on page 114
    set use-stmps {enable | disable} on page 115
    set webmail-language <language_name> on page 115
    set webmail-theme {IndigoDarkBlue | RedGrey | Standard | Use-System-Settings}
      on page 115
end
```

| Variable | Description | Default |
|---|---|---|
| addressbook {domain \| none \| system}<br>(server mode only) | Add newly created mail user to system address book, domain address book or not. | domain |
| bypass-bounce-verification {enable \| disable} | Enable to omit bounce address tag verification of email incoming to this protected domain.<br>This bypass does not omit bounce address tagging of outgoing email. | disable |
| fallback-host {<smtp-server_fqdn> \| <smtp-server_ipv4>}<br>(transparent mode and gateway mode only) | Enter the fully qualified domain name (FQDN) or IP address of the secondary SMTP server for this protected domain.<br>This SMTP server will be used if the primary SMTP server is unreachable. | |
| fallback-port <port_int><br>(transparent mode and gateway mode only) | Enter the port number on which the failover SMTP server listens.<br>If you enable Use SMTPS, Port automatically changes to the default port number for SMTPS, but can still be customized.<br>The default SMTP port number is 25; the default SMTPS port number is 465. | 25 |

| Variable | Description | Default |
|---|---|---|
| fallback-use-smtps {enable \| disable}<br>(transparent mode and gateway mode only) | Enable to use SMTPS for connections originating from or destined for this protected server. | disable |
| global-bayesian {enable \| disable} | Enable to use the global Bayesian database instead of the Bayesian database for this protected domain.<br>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.<br>Disable to use the per-domain Bayesian database.<br>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} | Specify how the FortiMail unit will identify itself during the `HELO` or `EHLO` greeting of outgoing SMTP connections that it initiates.<br>*domainname*: The FortiMail unit will identify itself using the domain name for this protected domain.<br>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.<br>*hostname*: The FortiMail unit will identify itself using its own host name.<br>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.<br>*othername*: If you select this option, another command `set other-helo-greeting <string>` will appear, allowing you enter a name other than the domain name or host name, for the HELO/EHELO greeating. | hostname |
| host <host_name><br>(transparent mode and gateway mode only) | The host name or IP address and port number of the mail exchanger (MX) for this protected domain.<br>If Relay Type is MX Record (this domain) or MX Record (alternative domain), this information is determined dynamically by querying the MX record of the DNS server, and this field will be empty. | |
| 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. | |

| Variable | Description | Default |
|---|---|---|
| | If you want to use the IP pool as the source IP address for this protected domain, according to the sender's email address in the envelope (`MAIL FROM:`), select the IP pool to use and select ***outgoing*** as the `ip-pool-direction`.<br>If you want to use the IP pool as the destination IP address (virtual host) for this protected domain, according to the recipient's email address in the envelope (`RCPT TO:`), select the IP pool to use and select *incoming* as the `ip-pool-direction`. You must also configure the MX record to direct email to the IP pool addresses as well.<br>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.<br>If you want to use the IP pool as both the destination and source IP address, select the IP pool to use and select *Both* as the `ip-pool-direction`.<br>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} | Sets the direction for the `ip-pool` option. See description above.<br>This option is only available after you configure the `ip-pool` option. | |
| 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.<br>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.<br>This option is available only when another protected domain exists to select as the parent domain. | disable |
| ldap-asav-profile <ldap-profile_name> | Specify the name of an LDAP profile which you have enabled and configured. | |
| 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.<br>If you enable `ldap-domain-routing-smtps`, this setting automatically changes to the default port number for SMTPS, but can still be customized.<br>The default SMTP port number is 25; the default SMTPS port number is 465.<br>This option is valid when `relay-type` is `ldap-domain-routing`. | 25 |

| Variable | Description | Default |
|---|---|---|
| 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> on page 108 and ldap-domain-routing-smtps {enable \|disable} on page 109.<br>This option is valid when `relay-type` is set to `ldap-domain-routing`. | |
| ldap-domain-routing-smtps {enable \|disable} | Enable to use SMTPS for connections originating from or destined for this protected server.<br>This option is valid when `relay-type` 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/disable LDAP mail routing. | 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.<br>Note: If both this option and `expire-inactivity <days_int>` on page 275 in the session profile are enabled, email size will be limited to whichever size is smaller. | 204800KB |
| other-helo-greeting <string> | After you set the `greeting-with-hostname` to `othername`, use this command to specify the name to use for HELO/EHELO greeting. | |
| port <smtp-port_int><br>(transparent mode and gateway mode only) | Set the SMTP port number of the mail server. | 25 |
| quarantine-report-schedule-status {enable \| disable} | Enable or disable domain-level quarantine report schedule setting.<br>The quarantine report settings for a protected domain are a subset of the system-wide quarantine report settings.<br>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 |

| Variable | Description | Default |
|---|---|---|
| quarantine-report-to-alt {enable \| disable} | Enable or disable sending domain-level quarantine report to a recipient other than the individual recipients or group owner. For example, you might delegate quarantine reports by sending them to an administrator whose email address is not locally deliverable to the protected domain, such as admin@lab.example.com. | disable |
| quarantine-report-to-alt-addr <recipient_email> | Enter the recipient's email address. | |
| quarantine-report-to-individual {enable \| disable} | Enable to send quarantine reports to all recipients. | enable |
| quarantine-report-to-ldap-groupowner {enable \| disable} | Enable to send quarantine reports to the LDAP group owner of the specified LDAP profile. | disable |
| 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.<br>`disable`: Do not verify that the recipient address is an email user account that actually exists.<br>`smtp`: Query the SMTP server using the SMTP RCPT command to verify that the recipient address is an email user account that actually exists. You can also choose to use the SMTP VRFY command to do the verification. This feature is available on the GUI when you create a domain.<br>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.<br>`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. | disable |

| Variable | Description | Default |
|---|---|---|
| | **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.<br><br>**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 \| 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.<br>`disable`: Do not verify that the recipient address is an email user account that actually exists.<br>`smtp`: Query the SMTP server to verify that the recipient address is an email user account that actually exists.<br>`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.<br>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.<br>**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.<br>**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-invalid-user-action {reject \| discard} | Action to take on invalid recipients. | reject |

| Variable | Description | Default |
|---|---|---|
| relay-type {host \| ip-pool \| ldap-domain-routing \| mx-lookup \| mx-lookup-alt-domain}<br>(transparent mode and gateway mode only) | Select from one of the following methods of defining which SMTP server will receive email from the FortiMail unit that is destined for the protected domain:<br>`host`: Configure the connection to one protected SMTP server or, if any, one fallback.<br>`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 223.<br>`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.<br>`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.<br>`ip-pool`: Configure the connection to rotate among one or many protected SMTP servers.<br>**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.<br>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.<br>Transparent mode: A private DNS server is required if both the FortiMail unit and the SMTP server are behind a NAT device such as a router or firewall. On the private DNS server, configure the protected SMTP server's A record with its private IP address. On the public DNS server, configure the protected SMTP server's A record with its public IP address. Do not modify the MX record. | host |
| remove-outgoing-received-header {enable \| disable} | Enable to remove the `Received:` message headers from email whose:<br>• sender email address belongs to this protected domain, and<br>• 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. | disable |

| Variable | Description | Default |
|---|---|---|
| | You can alternatively remove this header from any matching email using session profiles. | |
| sender-addr-rate-ctrl-max-msgs <integer> | 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 <integer> | 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 per sender per half an hour. | disable |
| sender-addr-rate-ctrl-state {enable \| disable} | Enable sender address rate control per sender email address. | disable |
| smtp-recipient-verification-command {rcpt \| vrfy}<br>(transparent mode and gateway mode only) | 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`.<br>For information about recipient verification, see `recipient-verification {disable \| ldap \| smtp} on page 110`<br>This option is only available after you select `smtp` in `recipient-verification`. | rcpt |
| smtp-recipient-verification-accept-reply-string <accept_string><br>(transparent mode and gateway mode only) | When FortiMail queries the SMTP server for recipient verification:<br>If the reply code of the VRFY command is 2xx, the recipient exists.<br>If the reply code is non-2xx, FortiMail will try to match the accept string you specified with the reply string. If the strings match, the recipient exists.<br>Otherwise, the recipient is unknown.<br>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.<br>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.<br>This command is available only when you set `SMTP-recipient-verification-command` to `vrfy`. | |
| tp-hidden {no \| yes}<br>(transparent mode only) | Enable to preserve the IP address or domain name of the SMTP client for incoming email messages in:<br>the SMTP greeting (`HELO`/`EHLO`) in the envelope and in the Received: message headers of email messages<br>the IP addresses in the IP header | no |

| Variable | Description | Default |
|---|---|---|
| | This masks the existence of the FortiMail unit to the protected SMTP server.<br>Disable to replace the SMTP client's IP address or domain name with that of the FortiMail unit.<br>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):<br>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<br>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<br>But if the option is disabled, the message headers would contain:<br>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<br>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<br>**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. | |
| tp-server-on-port <port_int><br>(transparent mode only) | Select the network interface (physical port) to which the protected SMTP server is connected.<br>Note: Selecting the wrong network interface will result in the FortiMail sending email traffic to the wrong network interface. | 0 |
| tp-use-domain-mta {yes \| no}<br>(transparent mode only) | Enable to proxy SMTP clients' incoming connections when sending outgoing email messages via the protected SMTP server.<br>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.<br>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.<br>This option does not affect incoming connections containing incoming email messages, which will always be handled by the built-in MTA.<br>Note: This option will be ignored for email that matches an antispam or content profile where you have enabled `alternate-host {<relay_fqdn> \| <relay_ipv4>}` on page 182. | no |

| Variable | Description | Default |
|---|---|---|
| use-stmps {enable \| disable} | Enable to use SMTPS to relay email to the mail server. | disable |
| webmail-language <language_name> | Select either ***Use system settings***, other language that the FortiMail unit will to display webmail and quarantine folder pages. By default, the FortiMail unit uses the same language as the web-based manager. | |
| webmail-theme {IndigoDarkBlue \| RedGrey \| Standard \| Use-System-Settings} | Select the display theme that the FortiMail unit will to display webmail and quarantine folder pages. By default, the FortiMail unit uses the same display theme as the web-based manager. | Use-System-Settings |

## config policy recipient

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

### Syntax

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

```
config policy recipient
   edit <policy_index> on page 116
      set auth-access-options {pop3 smtp-auth smtp-diff-identity web} on page 116
      set certificate-required {yes | no} on page 116
      set comment on page 116
      set direction on page 116
      set pkiauth {enable | disable} on page 116
      set pkiuser <user_name> on page 116
      set profile-antispam <antispam_name> on page 116
      set profile-antivirus <antivirus_name> on page 116
      set profile-auth-type {imap | local | ldap | pop3 | smtp | radius} on page
          116
      set profile-content <profile_name> on page 117
      set profile-dlp on page 117
      set profile-resource <profile_name> on page 117
      set profile-ldap <profile_name> on page 117
      set recipient-domain <domain> on page 117
      set recipient-name <name_str> on page 117
      set recipient-type {ldap-group | local-group | user} on page 117
      set sender-domain <domain_name> on page 117
      set sender-name <local-part_str> on page 118
      set sender-type {ldap-group | local-group | user} on page 118
      set smtp-diff-identity on page 118
      set smtp-diff-identity on page 118
      set smtp-diff-identity-lsap-profile on page 118
      set status {enable | disable} on page 118
   next
end
```

| Variable | Description | Default |
|---|---|---|
| <policy_index> | Type the index number of the policy.<br>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:<br>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.<br>web: Allow the email user to use FortiMail webmail (HTTP or HTTPS) to retrieve the contents of their per-recipient spam quarantine.<br>pop3: Allow the email user to use POP3 to retrieve the contents of their per-recipient spam quarantine.<br>smtp-auth: Use the authentication server selected in the authentication profile when performing SMTP authentication for connecting SMTP clients.<br>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}<br>(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}<br>(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><br>(transparent and gateway mode only) | Enter the name of the PKI user entry, or select a user you defined before.<br>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.<br>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. | |
| 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.<br>For example:<br>`set profile-auth-type ldap` | |

| Variable | Description | Default |
|---|---|---|
| | `set profile-auth-ldap ldap_profile1` | |
| profile-auth-imap <imap_name> | Type the name of an IMAP authentication profile.<br>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}` on page 116 | |
| profile-auth-ldap <ldap_name> | Type the name of an LDAP authentication profile.<br>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}` on page 116 | |
| profile-auth-pop3 <pop3_name> | Type the name of a POP3 authentication profile.<br>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}` on page 116 | |
| profile-auth-smtp <smtp_name> | Type the name of an SMTP authentication profile.<br>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}` on page 116. | |
| profile-auth-radius <radius_name> | Type the name of a RADIUS authentication profile.<br>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}` on page 116. | |
| 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.<br>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.<br>`user`: Select this option and then use the above command to enter the local part of the recipient email address.<br>`local-group`: Select this option and then specify the local group under this domain.<br>`ldap-group`: Select this option and then select an LDAP profile. | user |
| sender-domain <domain_name> | Enter the domain part of the sender email address. For example, example.com. | |

| Variable | Description | Default |
|---|---|---|
| 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.<br>`user`: Select this option and then use the above command to enter the local part of the sender email address.<br>`local-group`: Select this option and then specify the local group under this domain.<br>`ldap-group`: Select this option and then select an LDAP profile.<br>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-lsap-profile | Ldap profile for smtp sender identity verification. | |
| status {enable \| disable} | Enable or disable the policy. | enable |

## config profile account-sync

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 account-sync
   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-secondry-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`.<br>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.<br>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 |
| 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. | |

| Variable | Description | Default |
|---|---|---|
| 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. Set the value between 60-600. | 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-secondry-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_username> on page 120 to <new_username> on page 121 (see the note
        below)
   edit <user_name> on page 121
      set type {local | ldap} on page 121
      set type local
      set displayname <name_str> on page 121
      set password <pwd_str> on page 121
      set type ldap
      set displayname <name_str> on page 121
      set ldap-profile <ldap_name> on page 121
   next
end
```

| Variable | Description | Default |
|---|---|---|
| <old_username> | The user account name you want to rename. | |

| Variable | Description | Default |
|---|---|---|
| <new_ username> | The new user account name you want to change to. | |
| <user_name> | Enter the user name of an email user, such as `user1`. This is also the local-part portion of the email user's primary email address. | |
| type {local \| ldap} | Enter the type of email user account you want to add.<br>See set type local on page 120 and set type ldap on page 120. | ldap |
| displayname <name_str> | Enter the display name of the local email user, such as `'User One'`. | |
| password <pwd_ str> | Enter the password of the local email user. | |
| displayname <name_str> | Enter the display name of the LDAP email user, such as `'User One'`. | |
| ldap-profile <ldap_name> | Enter the name of an LDAP profile in which authentication queries are enabled. | |

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.

## 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.

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

Alternatively, you can configure LDAP queries to automatically add domain associations. For details, see system link-monitor on page 305.

## Syntax

```
config domain-association
   edit <domain-association-fqdn> on page 122
      set main-domain <protected-domain-name> on page 122
   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 on page 305

# file content-disarm-reconstruct

Attachments may contain potentially hazardous tags and attributes, such as hyperlinks and scripts. FortiMail provides the ability to remove or neutralize these hazardous contents and reconstruct the attachment files.

## Syntax

```
config file content-disarm-reconstruct
   set component-type-options {...}
   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 {...} | Enter the potentially hazardous content you wish to remove or neutralize from attachment files:<br>• office-action<br>• office-dde | |

| Variable | Description | Default |
|---|---|---|
| | • office-embedded-object<br>• office-hyperlink<br>• office-linked-object<br>• office-macro<br>• pdf-action-form<br>• pdf-action-gotor<br>• pdf-action-javascript<br>• pdf-action-launch<br>• pdf-action-movie<br>• pdf-action-sound<br>• pdf-action-uri<br>• pdf-embedded-file<br>• pdf-hyperlink<br>• pdf-javascript | |
| continue-sandbox-on-cdr {enable \| disable} | Enable or disable continuing the FortiSandbox scan on successful content disarm and reconstruct (CDR).<br>Note that when FortiMail is running firmware 6.4, even on successful CDR, FortiSandbox scanning for this attachment will **not** be bypassed.<br>When FortiMail is running firmware 7.0, the FortiSandbox scan on successful content disarm is bypassed by default. Enable `continue-sandbox-on-cdr` if you want to allow FortiSandbox to scan the attachment upon successful CDR. | disable |
| deferred-scan-notification-option {disarm \| remove} | Either send notification email with disarmed attachment or with the attachment removed. | 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 |
| modification-notice-option {enable \| disable} | Enable or disable appending the CDR disclaimer "Attachment has been reconstructed" for cleaned attachments. | disable |

# 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> on page 124
      set password <string> on page 124
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> on page 124
      set description <string> on page 124
      set extension <string> on page 124
      set mime-type <string> on page 124
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.<br>For example, to filter by image, and specifically for PNG, enter the following:<br>`set mime-type image/png`<br>To filter for all video formats, enter the following:<br>`set mime-type video/*` | |

# file signature

If you already have the SHA-1 (Secure Hash Algorithm 1) hash values of some known virus-infected files, you can add these values as file signatures and then, in the antivirus profile, enable the actions against these files. Use this command to add or edit the file signatures.

## Syntax

```
config file signature
   edit <signature_type> on page 125
      config item <hexadecimal>
         edit <signature_value>
      next
      set comments <string> on page 125
      set status {enable | disable} on page 125
      set type {sha1 | sha256} on page 125
end
```

| Variable | Description | Default |
|---|---|---|
| <signature_type> | Enter the file signature ID. | |
| comments <string> | Enter the general comments for the file signature. | |
| status {enable \| disable} | Enable or disable the signature check. | enable |
| type {sha1 \| sha256} | Enter the type of signature. | sha1 |

# 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_index> on page 126
      set certificate <certificate>
      set comma-separated-value {enable | disable} on page 126
      set encryption-log-status {enable | disable} on page 126
      set event-log-category {admin configuration ha | imap pop3 smtp system
          update webmail} on page 126
      set event-log-status {enable | disable} on page 126
      set facility {alert | audit | auth | authpriv | clock | cron | daemon |
          ftp | kern | local0 | local1 | local2 | local3 | local4 | local5 |
          local6 | local7 | lpr | mail | news | ntp} on page 127
      set history-log-status {enable | disable} on page 127
      set loglevel {alert | critical | debug | emergency | error | information |
          notification | warning} on page 127
      set matched-session-status {enable | disable}
      set port <port_int> on page 127
```

```
        set protocol {syslog | cftps} on page 127
        set server <log_ipv4> on page 127
        set spam-log-status {enable | disable} on page 127
        set status {enable | disable} on page 127
        set sysevent-log-category {admin | configuration | dns | ha | system |
             update}
        set sysevent-log-status {enable | disable}
        set syslog-mode {tcp | tcp-tls | udp}
        set virus-log-status {enable | disable} on page 127
end
```

| Variable | Description | Default |
|---|---|---|
| <log-destination_index> | Type an index number to identify which remote Syslog server or FortiAnalyzer unit you are configuring. | |
| certificate <certificate> | The certificate used by the Syslog-TLS connection to encrypt the log before delivery to the remote Syslog server.<br>This option is only available when `syslog-mode` is set to `tcp-tls`. | |
| comma-separated-value {enable \| disable} | Enable if you want to send log messages in comma-separated value (CSV) format.<br>**Note**: Do not enable this option if the log destination is a FortiAnalyzer unit. FortiAnalyzer units do not support CSV format logs. | disable |
| encryption-log-status {enable \| disable} | Enable or disable IBE event logging to a remote Syslog server or FortiAnalyzer unit. | disable |
| event-log-category {admin configuration ha \| imap pop3 smtp system update webmail} | Type all of the log types and subtypes that you want to record to this storage location. Separate each type with a space.<br>• `admin`: Log all administrative events, such as logins, resets, and configuration updates.<br>• `configuration`: Enable to log configuration changes.<br>• `ha`: Log all high availability (HA) activity.<br>• `imap`: Log all IMAP events.<br>• `pop3`: Log all POP3 events.<br>• `smtp`: Log all SMTP relay or proxy events.<br>• `system`: Log all system-related events, such as rebooting the FortiMail unit.<br>• `update`: Log both successful and unsuccessful attempts to download FortiGuard updates.<br>• `webmail`: Log all FortiMail webmail events. | |
| event-log-status {enable \| disable} | Enable or disable event logging to a remote Syslog server or FortiAnalyzer unit. | disable |

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

## Related topics

log setting local on page 128
log alertemail recipient on page 130

log alertemail setting on page 131

# log setting local

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

## Syntax

```
config log setting local
   set antispam-log-status {enable | disable} on page 128
   set antivirus-log-status {enable | disable} on page 128
   set disk-full {overwrite | nolog} on page 128
   set encryption-log-status {enable | disable} on page 128
   set event-log-category {admin configuration ha | imap pop3 smtp system update
        webmail} on page 128
   set event-log-status {enable | disable} on page 129
   set history-log-status {enable | disable} on page 129
   set loglevel {alert | critical | debug | emergency | error | information |
        notification | warning} on page 129
   set retention-period <days> on page 129
   set rotation-hour <hour_int> on page 129
   set rotation-period <days_int> on page 129
   set rotation-size <file-size_int> on page 129
   set status {enable | disable} on page 129
   set sysevent-log-category {admin | configuration | dns | ha | system | update}
        on page 129
   set system-event-log-status on page 129
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:<br>• `overwrite`: Delete the oldest log file in order to free disk space, and store the new log message.<br>• `nolog`: Discard the new log message. | overwrite |
| encryption-log-status {enable \| disable} | Enable to log all IBE events. | enable |
| event-log-category {admin configuration ha \| imap pop3 smtp system update webmail} | Type all of the log types and subtypes that you want to record to this storage location. Separate each type with a space.<br>`admin`: Log all administrative events, such as logins, resets, and configuration updates.<br>`configuration`: Enable to log configuration changes. | webmail smtp |

| Variable | Description | Default |
|---|---|---|
| | `ha`: Log all high availability (HA) activity.<br>`imap`: Log all IMAP events.<br>`pop3`: Log all POP3 events.<br>`smtp`: Log all SMTP relay or proxy events.<br>`system`: Log all system-related events, such as rebooting the FortiMail unit.<br>`update`: Log both successful and unsuccessful attempts to download FortiGuard updates.<br>`webmail`: Log all FortiMail webmail events. | |
| 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 |
| loglevel {alert \| critical \| debug \| emergency \| error \| information \| notification \| warning} | Type one of the following severity levels:<br>• `emergency`<br>• `alert`<br>• `critical`<br>• `error`<br>• `warning`<br>• `notification`<br>• `information`<br>• `debug`<br>This log destination will receive log messages greater than or equal to this severity level. | information |
| retention-period <days> | Specify how long to keep the logs. Valid rang is 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.<br>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). The valid range is between 1 to 500.<br>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 |
| sysevent-log-category {admin \| configuration \| dns \| ha \| system \| update} | Enter the system event log category to log. | configuration admin system ha update dns |
| system-event-log-status | Enable to log system events. | enable |

## Related topics

- log setting remote on page 125
- log alertemail recipient on page 130
- log alertemail setting on page 131

# 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 131.

## Syntax

```
config log alertemail recipient
   edit <recipient_email> on page 130
   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 on page 125
- log setting local on page 128
- log alertemail setting on page 131

# 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 130.

## 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} on page 131
   set deferq-interval <interval_int> on page 131
   set deferq-trigger <trigger_int> on page 131
   set license-interval <integer> on page 131
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:<br>• `deferq-over-limit`: The deferred mail queue has exceeded the number of messages during the interval specified in deferq-interval <interval_int> on page 131 and deferq-trigger <trigger_int> on page 131.<br>• `diskfull`: The FortiMail unit's hard disk is full.<br>• `ha`: A high availability (HA) event such as failover has occurred.<br>• `license-expire`: The license has expired.<br>• `remote-storage-failure`: Email archiving to the remote host has failed.<br>• `system`: The FortiMail unit has detected a system error.<br>• `system-quota-full`: The FortiMail unit has reached its disk space quota.<br>• `user-quota-full`: An email user account has reached its disk space quota.<br>• `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 |
| 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 on page 125
log setting local on page 128
log alertemail recipient on page 130

# 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} on page 132
   set email-addr-parsing-mode {strict | relaxed} on page 132
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.<br>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> on page 133
      set name <name_string> on page 133
      set mapped-host <host_name_string> on page 133
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 on page 125
log setting local on page 128
log alertemail recipient on page 130

# mailsetting mail-scan-options

Use this command to configure how to scan the compressed files.

## Syntax

```
config mailsetting mail-scan-options
   set content-scan-level {high | low | medium}
   set decompress-max-level <level_int> on page 134
   set decompress-max-size <size_in_MB> on page 134
   set scan-microsoft-msg {enable | disable}
   set scan-timeout-action {tempfail | passthrough} on page 134
   set scan-timeout-value <time-in-seconds> on page 134
end
```

| Variable | Description | Default |
|---|---|---|
| content-scan-level {high \| low \| medium} | Set the scan level of dictionary and DLP rules.<br>When set to `medium` or `high`, FortiMail carries out regex recursive matching, which consumes more 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 |
| decompress-max-size <size_in_MB> | Specify the maximum file size to scan after the archived files are decompressed. This applies to every single file after decompression. Bigger files will not be scanned. | 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 <time-in-seconds> | Specify how long in seconds FortiMail should spend on scanning email contents. The valid range is 270 to 900.<br>When the specified timeout has been reached, FortiMail will take the action specified above. | 285 |

## Related topics

mailsetting relay-host-list on page 137
mailsetting storage central-quarantine on page 141
mailsetting storage central-quarantine on page 141
mailsetting systemquarantine on page 144

# mailsetting preference

When you configure antispam, antivirus, and content action profiles, you may use the following actions:

- Deliver to alternate host
- Deliver to original host
- System quarantine
- Personal quarantine

For the above actions, you can choose to deliver or quarantine the original email or the modified email. For example, when the HTML content is converted to text, if you choose to deliver the unmodified copy, the HTML version will be delivered; if you choose to deliver the modified copy, the plain text version will be delivered.

## Syntax

```
config mailsetting preference
   set deliver-to-alternate-host {modified_copy | unmodified_copy} on page 135
   set deliver-to-original-host {modified_copy | unmodified_copy} on page 135
   set disclaimer-insertion {selected-message | all-message}
   set domain-quarantine {modified_copy | unmodified_copy}
   set enforce-delivery {enable | disable} on page 135
   set personal-quarantine {modified_copy | unmodified_copy} on page 135
   set personal-quarantine-attachment-scan {enable | disable} on page 135
   set subject-tag-location {beginning | end}
   set system-quarantine {modified_copy | unmodified_copy} on page 136
end
```

| Variable | Description | Default |
|---|---|---|
| deliver-to-alternate-host {modified_copy \| unmodified_copy} | Specify to use the modified email or the unmodified email. | modified_copy |
| deliver-to-original-host {modified_copy \| unmodified_copy} | Specify to use the modified email or the unmodified email. | modified_copy |
| disclaimer-insertion {selected-message \| all-message} | Define the email disclaimer insertion preference:<br>• `selected-message`: Disclaimer will not be added once again if the email is part of the existing email thread.<br>• `all-message`: Disclaimer will always be added, whether the email is a reply or a new email. | selected-message |
| domain-quarantine {modified_copy \| unmodified_copy} | Specify to use the modified email or the unmodified email. | modified_copy |
| enforce-delivery {enable \| disable} | Enforce delivery action if delivery to original/alternative host is enabled. | enable |
| personal-quarantine {modified_copy \| unmodified_copy} | Specify to use the modified email or the unmodified email. | modified_copy |
| personal-quarantine-attachment-scan {enable \| disable} | Enable or disable attachment scan for personal quarantined spam messages. | disable |

| Variable | Description | Default |
|---|---|---|
| subject-tag-location {beginning \| end} | Select where to insert the subject tag. | beginning |
| system-quarantine {modified_copy \| unmodified_copy} | Specify to use the modified email or the unmodified email. | modified_copy |

# 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} on page 136
end
```

| Variable | Description | Default |
|---|---|---|
| proxy-original {enable \| disable} | Enable to, for outgoing SMTP connections, use the outgoing proxy instead of the built-in MTA.<br>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.<br>Disable to relay email using the built-in MTA to either the SMTP relay defined in mailsetting relay-host-list on page 137, 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*.<br>Disclaimer messages require that this option be enabled. For more information, see system disclaimer on page 269.<br>  <br>If this option is enabled, consider also enabling session-prevent-open-relay {enable \| disable} on page 245. Failure to do so could allow clients to use open relays. | disable |

| Variable | Description | Default |
|---|---|---|
| | **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.<br>**Note**: If this option is enabled, you will not be able to use IP pools. For more information, see profile ip-pool on page 215.<br>**Note**: For security reasons, this option does not apply if there is no session profile selected in the applicable IP-based policy. For more information on configuring IP policies, see config policy delivery-control on page 159. | |

## Related topics

mailsetting relay-host-list on page 137
mailsetting storage central-quarantine on page 141
mailsetting storage central-quarantine on page 141
mailsetting systemquarantine on page 144

# 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 configure the FortiMail unit's built-in MTA's connection to an SMTP relay, if any, to which the FortiMail unit will relay outgoing email. You can configure up to eight relays.

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

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

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

You can also use MX records and IP groups as relay types.

For details, see the FortiMail Administration Guide.

This option will be ignored for email that matches an antispam or content profile where you have enabled `alternate-host {<relay_fqdn> | <relay_ipv4>} on page 182`.

## Syntax

```
config mailsetting relay-host-list
  edit <relay-host-name> on page 138
    set auth-password <password_str> on page 138
    set auth-status {enable | disable} on page 138
    set auth-type {auto | plain | login | digest-md5 | cram-md5} on page 138
    set auth-username <user_str> on page 139
    set host-name on page 139
    set host-port on page 139
    set ip-group-profile on page 139
    set mx-lookup-domain-name on page 139
    set relay-type {host | ip-group | mx-lookup} on page 139
    set use-smtps {enable | disable} on page 139
  end
```

| Variable | Description | Default |
|---|---|---|
| <relay-host-name> | Enter the host name or IP address of the relay server. | |
| auth-password <password_str> | If auth-status {enable \| disable} on page 138 is `enable`, enter the password of the FortiMail unit's user account on the SMTP relay. | |
| auth-status {enable \| disable} | Enable if the SMTP relay requires authentication using the SMTP `AUTH` command. Also configure `auth-username <user_str> on page 139`, `auth-password <password_str> on page 138`, and `auth-type {auto \| plain \| login \| digest-md5 \| cram-md5} on page 138`. | disable |
| auth-type {auto \| plain \| login \| digest-md5 \| cram-md5} | If auth-status {enable \| disable} on page 138 is `enable`, enter either the SMTP authentication type required by the SMTP relay when the FortiMail unit sends the ESMTP `AUTH` command, or enter `auto` to automatically detect and use the most secure authentication type supported by the relay server. | auto |

| Variable | Description | Default |
|---|---|---|
| auth-username <user_str> | If auth-status {enable \| disable} on page 138 is `enable`, enter the name of the FortiMail unit's user account on the SMTP relay. | |
| host-name | Enter the relay host ip or host name. | |
| host-port | Enter the host port number. | 25 |
| ip-group-profile | Enter an IP group profile. | |
| mx-lookup-domain-name | Enter the domain name for MX record lookup. | |
| relay-type {host \| ip-group \| mx-lookup} | Enter the SMTP relay type: host, ip-group, or mx-lookup. | host |
| use-smtps {enable \| disable} | Enable to initiate SSL- and TLS-secured connections to the SMTP relay if it supports SSL/TLS.<br>When disabled, SMTP connections from the FortiMail unit's built-in MTA or proxy to the relay will occur as clear text, unencrypted.<br>This option must be enabled to initiate SMTPS connections. | disable |

## Related topics


mailsetting proxy-smtp on page 136

mailsetting storage central-quarantine on page 141

mailsetting storage central-quarantine on page 141

mailsetting systemquarantine on page 144


# 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 `MAIL FROM:`, which is the FortiMail default setting for SMTP recipient verification. Use this command to add an envelope from address to solve the problem.

## Syntax

```
config mailsetting smtp-rcpt-verification
   set connection-type {auto | regular | secure}
   set mail-from-addr <email_address> on page 140
   set mode {regular | fail-open}
end
```

| Variable | Description | Default |
|---|---|---|
| connection-type {auto \| regular \| secure} | Define the connection type for SMTP recipient verification:<br>• `auto`: Attempt ESMTP protocol first, and fallback to SMTP protocol. ESMTP supports recipient verification for TLS-enforced backend connections.<br>• `regular`: Use SMTP protocol (HELO without STARTTLS).<br>• `secure`: Use ESMTP protocol (EHLO with STARTTLS). | regular |
| mail-from-addr <email_address> | Specify the envelope `MAIL FROM:` address to use. | |
| mode {regular \| fail-open} | Define the recipient verification mode:<br>• `regular`: Always perform recipient verification with the SMTP server.<br>• `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} on page
      141
  set client-ip <client_ipv4> on page 141
  set server-host <server_ipv4> on page 141
  set server-name <name_str> on page 141
end
```

| Variable | Description | Default |
|---|---|---|
| remote-storage-type {disable \| from-client \| to-server-over-ssl} | Enter one of the following centralized IBE types:<br>• `disable`: Centralized IBE storage is disabled. The FortiMail unit stores its IBE messages locally, on its own hard disks.<br>• `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 the high-end FortiMail models (FortiMail 1000D and above).<br>• `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 |
| client-ip <client_ipv4> | This option applies only if `remote-storage-type` is set to `from-client`.<br>Enter the IP address of the FortiMail unit that is allowed to store its IBE email on this high-end FortiMail unit.<br>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`.<br>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`.<br>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 | unknown} on page 142
   set client-ip <client_ipv4> on page 142
   set server-host <server_ipv4> on page 142
   set server-name <name_str> on page 142
end
```

| Variable | Description | Default |
|---|---|---|
| remote-storage-type {disable \| from-client \| to-server-over-ssl \| to-server-plain \| unknown} | Enter one of the following centralized quarantine types:<br>• `disable`: Centralized quarantine storage is disabled. The FortiMail unit stores its quarantines locally, on its own hard disks.<br>• `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 the high-end FortiMail models (FortiMail 1000D and above).<br>• `to-server-over-ssl`: Same as `to-server-plain`, except the connection uses SSL.<br>• `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.<br>• `unknown`: Centralized quarantine storage is unknown. | disable |
| client-ip <client_ipv4> | This option applies only if `remote-storage-type` is set to `from-client`.<br>Enter the IP address of the FortiMail unit that is allowed to store its quarantined email on this high-end FortiMail unit.<br>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`.<br>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`.<br>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 on page 136
mailsetting relay-host-list on page 137

mailsetting storage central-quarantine on page 141
mailsetting systemquarantine on page 144
mailsetting storage central-quarantine on page 141

# 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 on page 143
   set folder <folder_str> on page 143
   set host <host_str> on page 143
   set iscsi-id <id_str> on page 143
   set iscsi-use-initiator {enable | disable}
   set nfs-version {auto | nfs-v3 | nfs-v4} on page 144
   set password <password_str> on page 144
   set port <port_int> on page 144
   set protocol {nfs | iscsi_server} on page 144
   set type {local | remote} on page 144
   set username <user-name_str> on page 144
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.<br>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.<br>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).<br>Applies only when `protocol` is `iscsi_server`. | |
| iscsi-use-initiator {enable \| disable} | Enable to use ISCSI initiator name as username. | disable |

| Variable | Description | Default |
|---|---|---|
| nfs-version (auto \| nfs-v3 \| nfs-v4} | Use this command to control supported NFS versions.<br>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.<br>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:<br>• `nfs`: A network file system (NFS) server. If you select this option, enter the following information:<br>• `iscsi_server`: An Internet SCSI (Small Computer System Interface), also called iSCSI, server. If you select this option, enter the following information: | nfs |
| type {local \| remote} | Select whether to store email locally or on an NFS server. | local |
| username <user-name_ str> | Enter the user name of the FortiMail unit's account on the ISCSI server.<br>Applies only when `protocol` is `iscsi_server`. | |

## Related topics

mailsetting proxy-smtp on page 136
mailsetting relay-host-list on page 137
mailsetting storage central-quarantine on page 141
mailsetting systemquarantine on page 144

# 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> on page 145
   set forward-address <recipient_str> on page 145
   set password <password_str> on page 145
   set rotation-period <day_integer> on page 145
   set rotation-status {enable | disable} on page 145
```

```
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 |
| 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.<br>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.<br>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 on page 136

mailsetting relay-host-list on page 137

mailsetting storage central-quarantine on page 141

mailsetting storage central-quarantine on page 141


# ms365 account

Use this command to connect to Microsoft 365 to access the user mailboxes. You must have domain administrator privileges to access Microsoft 365.

## Syntax

```
config ms365 account
   edit <name> on page 146
      config user-filter
         edit <name>
```

```
            set ad-group-attr {custom | displayname | mail}
            set ad-group-attr-name <string>
            set ad-group-attr-value <string>
            set email-group <group_name>
            set ldap-group <string>
            set ldap-profile <profile_name>
            set pattern <string>
            set status {enable | disable}
            set type {ad-group | email-group | imported-user | ldap-group | regex |
                wildcard}
        next
    end
    set application-id <string>
    set application-secret <password>
    set description <string> on page 146
    set service-endpoint {china | germany | global | us-dod | us-gov}
    set tenant <password> on page 147
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter the name of the account profile. | |
| ad-group-attr {custom \| displayname \| mail} | **Note:** This option is only available when `type` is set to `ad-group`.<br>Select the Azure AD group attribute. | displayname |
| ad-group-attr-name <string> | **Note:** This option is only available when `type` is set to `ad-group` and `ad-group-attr` is set to `custom`.<br>Enter the custom Azure AD group attribute name. | |
| ad-group-attr-value <string> | **Note:** This option is only available when `type` is set to `ad-group`.<br>Enter the Azure AD group attribute value. | |
| application-id <string> | Enter the application ID. | |
| application-secret <password> | Enter the application secret/password. | |
| description <string> | Enter a brief description of the account. | |
| email-group <group_name> | **Note:** This option is only available when `type` is set to `email-group`.<br>Select an email group. | |
| ldap-group <string> | **Note:** This option is only available when `type` is set to `ldap-group`.<br>Enter the LDAP group name. | |
| ldap-profile <profile_name> | **Note:** This option is only available when `type` is set to `ldap-group`.<br>Select an LDAP group profile. | |
| pattern <string> | **Note:** This option is only available when `type` is set to `regex` or `wildcard`.<br>Enter the user pattern. | |

| Variable | Description | Default |
|---|---|---|
| service-endpoint {china \| germany \| global \| us-dod \| us-gov} | Select a regional endpoint appropriate to your geographical location. | global |
| status {enable \| disable} | Enable or disable this user filter. | disable |
| tenant <password> | Enter the Microsoft 365 tenant credentials. | |
| type {ad-group \| email-group \| imported-user \| ldap-group \| regex \| wildcard} | Define the filter type as one of the following:<br>• `ad-group`: Azure AD group.<br>• `email-group`: Email group.<br>• `imported-user`: Imported internal or external user.<br>• `ldap-group`: LDAP group.<br>• `regex`: User as regular expression.<br>• `wildcard`: User as wildcard. | wildcard |

# ms365 policy

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

## Syntax

```
config ms365 policy
   edit <name>
      set account <account_name>
      set profile-antispam <name>
      set profile-antivirus <name>
      set profile-content <name>
      set profile-dlp <name>
      set recipient-ad-group-attr {custom | displayname | mail}
      set recipient-ad-group-attr-name <string>
      set recipient-ad-group-attr-value <string>
      set recipient-domain <string>
      set recipient-email-group <group_name>
      set recipient-ldap-profile <profile_name>
      set recipient-name <string>
      set recipient-pattern-regex <string>
      set recipient-type {ad-group | email-group | ldap-group | regex | wildcard}
      set sender-ad-group-attr {custom | displayname | mail}
      set sender-ad-group-attr-name <string>
      set sender-ad-group-attr-value <string>
      set sender-domain <string>
      set sender-email-group <group_name>
      set sender-ldap-profile <profile_name>
      set sender-name <string>
      set sender-pattern-regex <string>
      set sender-type {ad-group | email-group | external | internal | ldap-group |
          regex | wildcard}
      set source-ip-address <ipv4mask>
```

```
        set source-type {geoip-group | ip-address | ip-group}
        set status {enable | disable}
    end
```

| Variable | Description | Default |
|---|---|---|
| account <account_name> | Select a Microsoft 365 account. | |
| profile-antispam <name> | Assign an antispam profile to the real-time scan policy. | |
| profile-antivirus <name> | Assign an antivirus profile to the real-time scan policy. | |
| profile-content <name> | Assign an content profile to the real-time scan policy. | |
| profile-dlp <name> | Assign an DLP profile to the real-time scan policy. | |
| recipient-ad-group-attr {custom \| displayname \| mail} | **Note:** This option is only available when `recipient-type` is set to `ad-group`.<br>Select the recipient Azure AD group attribute. | displayname |
| recipient-ad-group-attr-name <string> | **Note:** This option is only available when `recipient-type` is set to `ad-group` and `recipient-ad-group-attr` is set to `custom`.<br>Enter the custom recipient Azure AD group attribute name. | |
| recipient-ad-group-attr-value <string> | **Note:** This option is only available when `recipient-type` is set to `ad-group`.<br>Enter the recipient Azure AD group attribute value. | |
| recipient-domain <string> | Domain part of recipient email address. | |
| recipient-email-group <group_name> | **Note:** This option is only available when `recipient-type` is set to `email-group`.<br>Select an email group. | |
| recipient-ldap-profile <profile_name> | **Note:** This option is only available when `recipient-type` is set to `ldap-group`.<br>Select an LDAP group profile. | |
| recipient-name <string> | **Note:** This option is only available when `recipient-type` is set to `wildcard`.<br>Local part of recipient email address. | |
| recipient-pattern-regex <string> | **Note:** This option is only available when `recipient-type` is set to `regex`.<br>Enter the sender email address regular expression pattern. | |
| recipient-type {ad-group \| email-group \| ldap-group \| regex \| wildcard} | Define the recipient as one of the following:<br>• `ad-group`: Azure AD group.<br>• `email-group`: Email group.<br>• `ldap-group`: LDAP group.<br>• `regex`: User as regular expression.<br>• `wildcard`: User as wildcard. | wildcard |
| sender-ad-group-attr {custom \| displayname \| mail} | **Note:** This option is only available when `sender-type` is set to `ad-group`.<br>Select the sender Azure AD group attribute. | displayname |

| Variable | Description | Default |
|---|---|---|
| sender-ad-group-attr-name <string> | **Note:** This option is only available when `sender-type` is set to `ad-group` and `sender-ad-group-attr` is set to `custom`.<br>Enter the custom sender Azure AD group attribute name. | |
| sender-ad-group-attr-value <string> | **Note:** This option is only available when `sender-type` is set to `ad-group`.<br>Enter the sender Azure AD group attribute value. | |
| sender-domain <string> | Domain part of sender email address. | |
| sender-email-group <group_name> | **Note:** This option is only available when `sender-type` is set to `email-group`.<br>Select an email group. | |
| sender-ldap-profile <profile_name> | **Note:** This option is only available when `sender-type` is set to `ldap-group`.<br>Select an LDAP group profile. | |
| sender-name <string> | **Note:** This option is only available when `sender-type` is set to `wildcard`.<br>Local part of sender email address. | |
| sender-pattern-regex <string> | **Note:** This option is only available when `sender-type` is set to `regex`.<br>Enter the recipient email address regular expression pattern. | |
| sender-type {ad-group \| email-group \| external \| internal \| ldap-group \| regex \| wildcard} | Define the sender as one of the following:<br>• `ad-group`: Azure AD group.<br>• `email-group`: Email group.<br>• `external`: External sender.<br>• `internal`: Internal sender.<br>• `ldap-group`: LDAP group.<br>• `regex`: User as regular expression.<br>• `wildcard`: User as wildcard. | wildcard |
| source-ip-address <ipv4mask> | Client IP address and netmask. | 0.0.0.0/0 |
| source-type {geoip-group \| ip-address \| ip-group} | Define the source as either GeoIP group, IP address and netmask, or IP group. | ip-address |
| status {enable \| disable} | Enable or disable the policy. | disable |

# ms365 profile action

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

## Syntax

```
config ms365 profile action
   edit <name> on page 146
      set final-action {discard | move | none | quarantine | quarantine-review} on
          page 150
      set move-to-folder-name <string>
      set notification-profile <profile-name> on page 150
      set notification-status {enable | disable} on page 150
      set replace-message <string> on page 150
      set replace-status {enable | disable} on page 150
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter the name of the action profile or create a new one. | |
| final-action {discard \| move \| none \| quarantine \| quarantine-review} | Enter one of the following final actions to perform on infected emails:<br>• `discard`: Move the email message from the user's inbox to the Junk folder on Microsoft 365.<br>• `move`: Move the email message from the user's inbox to a specified folder on Microsoft 365. See move-to-folder-name <string>.<br>• none: No action is taken.<br>• `quarantine`: Create a bulk folder for the user on Microsoft 365 and move the email message from the user's inbox to their Bulk folder.<br>• `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. | |
| move-to-folder-name <string> | 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 <string> | Enter the name of the custom message for content replacement. | default |
| replace-status {enable \| disable} | Enable or disable the content replacement. | disable |

# ms365 profile antispam

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

See profile antispam on page 169 for more details on commands and descriptions.

# ms365 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 domain.

See profile antivirus on page 185 for more details on commands and descriptions.

# ms365 profile bec

Use this command to configure business email compromise (BEC) profile rules for the administrator account of the Microsoft 365 domain. To avoid false positives and false negatives, assign scores to adjust the weight allocated to each of the most common BEC attack types, such as cousin domains, suspicious characters, sender alignment, action keywords, and URL categories.

Once configured, BEC profiles are then used in antispam profiles.

## Syntax

```
config profile bec
   edit <name>
      config rule
      set comment <string>
         edit <order-integer>
            set action <datasource>
            set action-keyword-score <float>
            set cousin-domain-score <float>
            set malformed-email-score <float>
            set name <string>
            set sender-alignment-score <float>
            set status {enable | disable}
            set suspicious-character-score <float>
            set threshold <float>
            set url-profile <datasource>
            set url-profile-score <float>
         next
      end
end
```

## Syntax

| Variable | Description | Default |
|---|---|---|
| action <datasource> | Enter an antispam action profile name for the rule. | |
| action-keyword-score <float> | Enter a weight-adjusted score for actions keywords. | 10.000000 |

| Variable | Description | Default |
|---|---|---|
| cousin-domain-score <float> | Enter a weight-adjusted score for cousin domains. | 10.000000 |
| malformed-email-score <float> | Enter a weight-adjusted score for malformed emails.<br>Malformed emails are those emails that contain malformed data in the email structure, header, or body. For more information, see RFC 7103. | 10.000000 |
| name <string> | Enter a name for the rule. | |
| sender-alignment-score <float> | Enter a weight-adjusted score for sender alignment.<br>Sender alignment checks for a Header From and Envelope From domain mismatch. | 10.000000 |
| status {enable \| disable} | Enable or disable the profile rule. | enable |
| suspicious-character-score <float> | Enter a weight-adjusted score for suspicious characters. | 10.000000 |
| threshold <float> | Define the threshold at which point actions are taken. This score is allocated to the other categories. | 50.000000 |
| url-profile <datasource> | Enter a URL profile to assign to the URL category (`url-profile-score`). | unrated |
| url-profile-score <float> | Enter a weight-adjusted score for URL profiles that analyze any phishing URLs contained within emails. | 10.000000 |

# ms365 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 on page 197 for more details on commands and descriptions.

# ms365 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 on page 211 for more details on commands and descriptions.

# ms365 setting

Use this command to configure real-time scan settings.

## Syntax

```
config ms365 setting
   set hide-email-on-arrival {enable | disable}
   set push-notification-url-base <string>
   set realtime-scan-log {all | on-policy-match}
   set realtime-scan-status {enable | disable}
   set service-endpoint {china | germany | global | us-dod | us-gov}
end
```

| Variable | Description | Default |
|---|---|---|
| hide-email-on-arrival {enable \| disable} | Enable or disable moving email to hidden folder on arrival for real-time scan.<br>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. | disable |
| push-notification-url-base <string> | Define the base URL to receive notifications. | |
| realtime-scan-log {all \| on-policy-match} | Enter a realtime scan log option. When set to `on-policy-match`, Microsoft 365 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 scan. | disable |
| service-endpoint {china \| germany \| global \| us-dod \| us-gov} | Enter the appropriate geographical Microsoft 365 service endpoint. | global |

# policy access-control receive

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

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

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

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

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

For protected domains, the default action is ***RELAY***.

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

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

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

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

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

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

Unlike IP-based policies, however, access control rules **cannot** affect email in ways that occur after the session's `DATA` command, such as by applying antispam profiles. Access control rules also cannot be overruled by recipient-based policies, and cannot match connections based upon the IP address of the SMTP server (by the nature of how the ACL controls access to or through the FortiMail unit, the SMTP server is always the FortiMail unit itself, **unless** the FortiMail unit is operating in transparent mode). For more information on IP-based policies, see the FortiMail Administration Guide.

## Syntax

```
config policy access-control receive
   edit <rule_id> on page 155
      set action {bypass | discard | reject | relay} on page 155
      set authenticated {any | authenticated | not-authenticated} on page 155
      set comment <string> on page 155
      set recipient-pattern <pattern_str> on page 155
      set recipient-pattern-type {default | group | regexp} on page 155
      set recipient-pattern-regexp {yes | no} on page 155
      set recipient-pattern-group <group_name> on page 155
      set reverse-dns-pattern <pattern_str> on page 155
      set reverse-dns-pattern-regexp {yes | no} on page 156
      set sender-ip-group <ip_group_name> on page 156
      set sender-ip-mask <ip&netmask_str> on page 156
      set sender-ip-type {ip-group | ip-mask} on page 156
      set sender-pattern <pattern_str> on page 156
      set sender-pattern-type {default | group | regexp} on page 156
      set sender-pattern-group <group_name> on page 157
      set sender-pattern-regexp {yes | no} on page 157
      set status {enable | disable} on page 157
      set tls-profile <profile_str> on page 157
end
```

| Variable | Description | Default |
|---|---|---|
| <rule_id> | Enter the number identifying the rule. | |
| action {bypass \| discard \| reject \| relay} | Enter the action the FortiMail unit will perform for SMTP sessions matching this access control rule.<br>`bypass`:Relay or proxy and deliver the email, **but**, if the sender or recipient belongs to a protected domain, bypass all antispam profile processing. Antivirus, content and other scans will still occur.<br>`discard`: Accept the email, but silently delete it and do not deliver it. Do not inform the SMTP client.<br>`reject`: Reject delivery of the email and respond to the SMTP client with SMTP reply code 550 (`Relaying denied`).<br>`relay`: Relay or proxy, process, and deliver the email normally if it passes all configured scans. | relay |
| authenticated {any \| authenticated \| not-authenticated} | Enter a value to indicate whether this rule applies only to messages delivered by clients that have authenticated with the FortiMail unit.<br>`any`: Match or do not match this access control rule regardless of whether the client has authenticated with the FortiMail unit.<br>`authenticated`: Match this access control rule only for clients that have authenticated with the FortiMail unit.<br>`not-authenticated`: Match this access control rule only for clients that have **not** authenticated with the FortiMail unit. | authenticated |
| comment <string> | Enter any comments for access control rules for receiving email. | |
| recipient-pattern <pattern_str> | Enter a pattern that defines recipient email addresses which match this rule, surrounded in slashes and single quotes (such as `\'*\'`). | * |
| recipient-pattern-type {default \| group \| regexp} | Enter the pattern type.<br>`default`: This is the user defined pattern. Also configure `recipient-pattern <pattern_str> on page 155`.<br>`group`: If you enter this option, configure `recipient-pattern-group <group_name> on page 155`.<br>`regexp`: If you enter this option, configure `recipient-pattern-regexp {yes \| no} on page 155`. | default |
| recipient-pattern-regexp {yes \| no} | Enter `yes` to use regular expression syntax instead of wildcards to specify the recipient pattern.<br>This option is available only when `recipient-pattern-type {default \| group \| regexp} on page 155` is `regexp`. | no |
| recipient-pattern-group <group_name> | Enter the group name to specify the recipient pattern.<br>This option is available only when `recipient-pattern-type {default \| group \| regexp} on page 155` is `group`. | |
| reverse-dns-pattern <pattern_str> | Enter a pattern to compare to the result of a reverse DNS look-up of the IP address of the SMTP client delivering the email message. | * |

| Variable | Description | Default |
|---|---|---|
| | Because domain names in the SMTP session are self-reported by the connecting SMTP server and easy to fake, the FortiMail unit does not trust the domain name that an SMTP server reports. Instead, the FortiMail does a DNS lookup using the SMTP server's IP address. The resulting domain name is compared to the reverse DNS pattern for a match. If the reverse DNS query fails, the access control rule match will also fail. If no other access control rule matches, the connection will be rejected with SMTP reply code 550 (`Relaying denied`).<br>Wildcard characters allow you to enter partial patterns that can match multiple reverse DNS lookup results. An asterisk (`*`) represents one or more characters; a question mark (`?`) represents any single character.<br>For example, the recipient pattern `mail*.com` will match messages delivered by an SMTP server whose domain name starts with "mail" and ends with ".com".<br>Note: Reverse DNS queries for access control rules require that the domain name be a valid top level domain (TLD). For example, ".lab" is not a valid top level domain name, and thus the FortiMail unit cannot successfully perform a reverse DNS query for it. | |
| reverse-dns-pattern-regexp {yes \| no} | Enter `yes` to use regular expression syntax instead of wildcards to specify the reverse DNS pattern. | no |
| sender-ip-group <ip_group_name> | Enter the IP group of the SMTP client attempting to deliver the email message.<br>This option only appears if you enter ip-group in `sender-ip-type {ip-group \| ip-mask}` on page 156. | |
| sender-ip-mask <ip&netmask_str> | Enter the IP address and netmask of the SMTP client attempting to deliver the email message. Use the netmask, the portion after the slash (`/`), to specify the matching subnet.<br>For example, enter `10.10.10.10/24` to match a 24-bit subnet, or all addresses starting with 10.10.10. This will appear as ***10.10.10.0/24*** in the access control rule table, with the `0` indicating that any value is matched in that position of the address.<br>Similarly, `10.10.10.10/32` will appear as 10.10.10.10/32 and match only the 10.10.10.10 address.<br>To match any address, enter `0.0.0.0/0`. | 0.0.0.0 0.0.0.0 |
| sender-ip-type {ip-group \| ip-mask} | Select the method of the SMTP client attempting to deliver the email message. Also configure `sender-ip-mask <ip&netmask_str>` on page 156 and `sender-ip-group <ip_group_name>` on page 156. | ip-mask |
| sender-pattern <pattern_str> | Enter a pattern that defines sender email addresses which match this rule, surrounded in slashes and single quotes (such as `\'*\'` ).<br>This option is only available if you enter `default` in `sender-pattern-type {default \| group \| regexp}` on page 156. | * |
| sender-pattern-type {default \| group \| regexp} | Enter the pattern type.<br>`default`: This is the user defined pattern. Also configure `sender-pattern <pattern_str>` on page 156. | default |

| Variable | Description | Default |
|---|---|---|
| | `group`: If you enter this option, configure `sender-pattern-group <group_name>` on page 157.<br>`regexp`: If you enter this option, configure `sender-pattern-regexp {yes \| no}` on page 157. | |
| sender-pattern-group <group_name> | Enter the group name to match any email address in the group.<br>This option is only available if you enter `group` in `sender-pattern-type {default \| group \| regexp}` on page 156. | |
| sender-pattern-regexp {yes \| no} | Enter `yes` to use regular expression syntax instead of wildcards to specify the sender pattern.<br>This option is only available if you enter `regexp` in `sender-pattern-type {default \| group \| regexp}` on page 156. | no |
| status {enable \| disable} | Enter `enable` to activate this rule. | enable |
| tls-profile <profile_str> | Enter a TLS profile to allow or reject the connection based on whether the communication session attributes match the settings in the TLS profile.<br>If the attributes match, the access control action is executed.<br>If the attributes do **not** match, the FortiMail unit performs the ***Failure*** action configured in the TLS profile.<br>For more information on TLS profiles, see the FortiMail Administration Guide. | |

## Related topics

policy access-control delivery on page 157
config policy delivery-control on page 159
policy recipient on page 163

# policy access-control delivery

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

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

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

## Syntax

```
config policy access-control delivery
   edit <rule_id> on page 158
      set comment <string> on page 158
      set destination <ip&netmask_str> on page 158
      set encryption-profile <profile_str> on page 158
      set ip-pool-profile on page 158
      set recipient-pattern <pattern_str> on page 158
      set sender-pattern <pattern_str> on page 158
      set status {enable | disable} on page 159
      set tls-profile <profile_str> on page 159
end
```

| Variable | Description | Default |
|---|---|---|
| <rule_id> | Enter the number identifying the rule. | |
| comment <string> | Enter any comments for email delivery rules. | |
| destination <ip&netmask_str> | Enter the IP address and netmask of the system to which the FortiMail unit is sending the email message. Use the netmask, the portion after the slash (/) to specify the matching subnet.<br>For example, enter `10.10.10.10/24` to match a 24-bit subnet, or all addresses starting with 10.10.10. This will appear as ***10.10.10.0/24*** in the access control rule table, with the `0` indicating that any value is matched in that position of the address.<br>Similarly, `10.10.10.10/32` will appear as ***10.10.10.10/32*** and match only the 10.10.10.10 address.<br>To match any address, enter `0.0.0.0/0`. | 0.0.0.0<br>0.0.0.0 |
| encryption-profile <profile_str> | Enter an encryption profile to apply identity-based encryption, if a corresponding sender identity exists in the certificate bindings.<br>For more information on encryption profiles, see the *FortiMail Administration Guide*. | |
| ip-pool-profile | Enter the name of the IP pool profile.<br>The IP pool profile will deliver incoming emails from FortiMail to the protected server. | |
| recipient-pattern <pattern_str> | Enter a complete or partial envelope recipient (`RCPT TO:`) email address to match.<br>Wild card characters allow you to enter partial patterns that can match multiple recipient email addresses. The asterisk (`*`) represents one or more characters and the question mark (`?`) represents any single character.<br>For example, the recipient pattern `*@example.???` will match messages sent to any email user at example.com, example.net, example.org, or any other “example" domain ending with a three-letter top-level domain name. | |
| recipient-pattern-type | Enter the type of recipient pattern. | |
| sender-pattern <pattern_str> | Enter a complete or partial envelope sender (`MAIL FROM:`) email address to match.<br>Wild card characters allow you to enter partial patterns that can match multiple sender email addresses. The asterisk (*) represents one or more characters and the question mark (?) represents any single character. | |

| Variable | Description | Default |
|---|---|---|
| | For example, the sender pattern `??@*.com` will match messages sent by any email user with a two letter email user name from any ".com" domain name. | |
| sender-pattern-type | Enter the type of the sender-pattern. | |
| status {enable \| disable} | Enter `enable` to activate this rule. | disable |
| tls-profile <profile_str> | Enter a TLS profile to allow or reject the connection based on whether the communication session attributes match the settings in the TLS profile.<br>If the attributes match, the access control action is executed.<br>If the attributes do **not** match, the FortiMail unit performs the ***Failure*** action configured in the TLS profile.<br>For more information on TLS profiles, see the *FortiMail Administration Guide*. | |

## Related topics

ms365 profile antivirus on page 151
config policy delivery-control on page 159
policy recipient on page 163

# policy delivery-control

Use this command to configure email delivery control options.

## Syntax

```
config policy delivery-control
   edit <delivery rule id>
      set max-concurrent-connection on page 159
      set max-messages-per-connection on page 159
      set max-recipients-per-message
      set max-recipients-per-period on page 160
      set recipient-domain on page 160
      set status {enable | disable} on page 160
end
```

| Variable | Description | Default |
|---|---|---|
| max-concurrent-connection | Enter the maximum concurrent SMTP connections (0 to disable). | |
| max-messages-per-connection | Enter the maximum messages per SMTP connection (0 to disable). | |

| Variable | Description | Default |
|---|---|---|
| max-recipients-per-message | Enter the maximum recipients per message (0 to disable). The valid range is 0-1000. | 100 |
| max-recipients-per-period | Enter the maximum recipients per period (0 to disable). | |
| recipient-domain | Enter the recipient domain. | |
| status {enable \| disable} | Enable the rule. | |
| file_name <file_str> | Enter the name of the language resource file, such as `'custom_french1'`. | |

# policy ip

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

## Syntax

```
config policy ip
   edit <policy_int> on page 160
      set action {proxy-bypass | reject | scan | temp-fail} on page 161
      set client-ip-group <group_name> on page 161
      set client <client_ipv4mask> on page 161
      set client-type {ip-address |ip-group | ip-pool} on page 161
      set comment on page 161
      set exclusive {enable | disable} on page 161
      set profile-antispam <antispam-profile_name> on page 161
      set profile-antivirus <antivirus-profile_name> on page 161
      set profile-auth-type {imap | ldap | none | pop3 | radius | smtp}
      set profile-content <content-profile_name> on page 161
      set profile-dlp on page 161
      set profile-ip-pool <ip-pool_name> on page 162
      set profile-session <session-profile_name> on page 162
      set server-ip-group <group_name> on page 162
      set server <smtp-server_ipv4mask> on page 162
      set server-ip-pool <ip-pool_str> on page 162
      set server-type {ip-address | ip-group | ip-pool} on page 162
      set smtp-diff-identity {enable | disable} on page 162
      set smtp-diff-identity-ldap on page 162
      set smtp-diff-identity-ldap-profile on page 162
      set status {enable | disable} on page 162
      set use-for-smtp-auth {enable | disable} on page 162
end
```

| Variable | Description | Default |
|---|---|---|
| <policy_int> | Enter the index number of the IP-based policy. | |

| Variable | Description | Default |
|---|---|---|
| action {proxy-bypass \| reject \| scan \| temp-fail} | Enter an action for this policy:<br>`Proxy-bypass`: Bypass the FortiMail unit's scanning. This action is for transparent mode only.<br>`scan`: Accept the connection and perform any scans configured in the profiles selected in this policy.<br>`reject`: Reject the email and respond to the SMTP client with SMTP reply code 550, indicating a permanent failure.<br>`Fail Temporarily`: Reject the email and respond to the SMTP client with SMTP reply code 451, indicating and indicate a temporary failure. | scan |
| client-ip-group <group_name> | Enter the IP group of the SMTP client to whose connections this policy will apply.<br>This option only appears if you enter `ip-group` in `client-type {ip-address \|ip-group \| ip-pool} on page 161`. | |
| client <client_ipv4mask> | Enter the IP address and subnet mask of the SMTP client to whose connections this policy will apply.<br>To match all clients, enter `0.0.0.0/0`. | 192.168.224.15<br>255.255.255.255 |
| client-type {ip-address \|ip-group \| ip-pool} | Enter the client type. | ip-address |
| comment | Enter a brief comment for the IP policy. | |
| 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.<br>Disable to apply any matching recipient-based policy in addition to the IP-based policy. Any profiles selected in the recipient-based policy will override those selected in the IP-based policy. | disable |
| profile-antispam <antispam-profile_name> | Enter the name of an outgoing antispam profile, if any, that this policy will apply. | |
| profile-antivirus <antivirus-profile_name> | Enter the name of an antivirus profile, if any, that this policy will apply. | |
| profile-auth-type {imap \| ldap \| none \| pop3 \| radius \| smtp} | Enter the type of the authentication profile that this policy will apply.<br>The command `profile-auth-<auth_type>` appears for the type chosen. Enter the name of an authentication profile for the type. | none |
| profile-content <content-profile_name> | Enter the name of the content profile that you want to apply to connections matching the policy. | |
| profile-dlp | Enter the name of the DLP profile for this policy. | |

| Variable | Description | Default |
|---|---|---|
| profile-ip-pool <ip-pool_name> | Enter the name of the IP pool profile that you want to apply to connections matching the policy. | |
| profile-session <session-profile_name> | Enter the name of the session profile that you want to apply to connections matching the policy. | |
| server-ip-group <group_name> | Enter the name of the IP group profile that you want to apply to connections matching the policy.<br>This option is only available when the `server-type` is `ip-group`. | |
| server <smtp-server_ipv4mask> | Enter the IP address and subnet mask of the SMTP server to whose connections this policy will apply.<br>To match all servers, enter `0.0.0.0/0`.<br>This option applies only for FortiMail units operating in transparent mode. For other modes, the FortiMail unit receives the SMTP connection, and therefore acts as the server. | 0.0.0.0<br>0.0.0.0 |
| server-ip-pool <ip-pool_str> | Enter the name of the ip pool to whose connections this policy will apply. This option is only available when the `server-type` is `ip-pool`. | |
| server-type {ip-address \| ip-group \| ip-pool} | Enter the SMTP server type o whose connections this policy will apply. Also configure `server <smtp-server_ipv4mask> on page 162`, `server-ip-group <group_name> on page 162`, and `server-ip-pool <ip-pool_str> on page 162`. | ip-address |
| 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.<br>Disable to require that the sender email address in the SMTP envelope match the authenticated user name. | disable |
| smtp-diff-identity-ldap | Verify SMTP sender identity with LDAP for authenticated email. | disable |
| smtp-diff-identity-ldap-profile | LDAP profile for SMTP sender identity verification. | disable |
| status {enable \| disable} | Enable to apply this policy. | enable |
| use-for-smtp-auth {enable \| disable} | Enable to authenticate SMTP connections using the authentication profile configured in sensitive-data {...} on page 102. | disable |

## Related topics

ms365 profile antivirus on page 151
policy access-control delivery on page 157
policy recipient on page 163

# 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> on page 163
      set auth-access-options {pop3 | smtp-auth | smtp-diff-identity | web} on
          page 163
      set certificate-required {yes | no} on page 164
      set comment <comment>
      set direction {incoming | outgoing}
      set pkiauth {enable | disable} on page 164
      set pkiuser <user_str> on page 164
      set profile-antispam <antispam-profile_name> on page 164
      set profile-antivirus <antivirus-profile_name> on page 164
      set profile-auth-type {imap | ldap | none | pop3 | radius | smtp} on page
          164
      set profile-content <content-profile_name> on page 164
      set profile-dlp <profile_name>
      set profile-ldap-recipient <ldap-profile_name>
      set profile-ldap-sender <ldap-profile_name>
      set profile-resource <profile_name>
      set recipient-domain <domain_str> on page 165
      set recipient-name <local-part_str> on page 165
      set recipient-pattern-regex <string>
      set recipient-type {email-address-group | ldap-group | regexp | user} on
          page 165
      set sender-domain <domain_str> on page 165
      set sender-name <local-part_str> on page 165
      set sender-pattern-regex <string>
      set sender-type {email-address-group | ldap-group | regexp | user} on page
          165
      set smtp-diff-identity {enable | disable} on page 165
      set smtp-diff-identity-ldap {enable | disable}
      set smtp-diff-identity-ldap-profile <profile_name>
      set status {enable | disable} on page 165
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.<br>pop3: Allow the email user to use POP3 to retrieve the contents of their per-recipient spam quarantine.<br>smtp-auth: Use the authentication server selected in the authentication profile when performing SMTP authentication for connecting SMTP clients. | |

| Variable | Description | Default |
|---|---|---|
| | `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.<br>`web`: Allow the email user to use FortiMail webmail (HTTP or HTTPS) to retrieve the contents of their per-recipient spam quarantine.<br>**Note:** Entering this option allows, but does not require, SMTP authentication. To enforce SMTP authentication for connecting SMTP clients, ensure that all access control rules require authentication. | |
| certificate-required {yes \| no} | If the email user's web browser does not provide a valid personal certificate, the FortiMail unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enter `yes`. | no |
| comment <comment> | Optionally, enter a comment for the recipient policy. | |
| direction {incoming \| outgoing} | Select the mail traffic direction. | 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. | disable |
| pkiuser <user_str> | If `pkiauth` is `enable`, enter the name of a PKI user, such as `'user1'`. For information on configuring PKI users, see user pki on page 330. | |
| profile-antispam <antispam-profile_name> | Enter the name of an antispam profile, if any, that this policy will apply. | |
| profile-antivirus <antivirus-profile_name> | Enter the name of an antivirus profile, if any, that this policy will apply. | |
| profile-auth-type {imap \| ldap \| none \| pop3 \| radius \| smtp} | Enter the type of the authentication profile that this policy will apply.<br>The command `profile-auth-<auth_type>` appears for the type chosen. Enter the name of an authentication profile for the type. | none |
| 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. | |
| profile-ldap-recipient <ldap-profile_name> | If `recipient-type` is `ldap-group`, enter the name of an LDAP profile in which the group owner query has been enabled and configured. | |

| Variable | Description | Default |
|---|---|---|
| profile-ldap-sender <ldap-profile_ name> | If `sender-type` is `ldap-group`, enter the name of an LDAP profile in which the group owner query has been enabled and configured. | |
| recipient-domain <domain_str> | Enter the domain part of recipient email address to define recipient (`RCPT TO:`) email addresses that match this policy. | |
| recipient-name <local-part_str> | Enter the local part of recipient email address to define recipient (`RCPT TO:`) email addresses that match this policy. | |
| recipient-pattern-regex <string> | Define the recipient email address regular expression pattern.<br>This option is only available when `recipient-type` is set to `regexp`. | .* |
| recipient-type {email-address-group \| ldap-group \| regexp \| user} | Enter one of the following ways to define recipient (`RCPT TO:`) email addresses that match this policy.<br>If you enter `ldap-group`, also configure `profile-ldap` by entering an LDAP profile in which you have enabled and configured a group query. | user |
| sender-pattern-regex <string> | Define the sender email address regular expression pattern.<br>This option is only available when `sender-type` is set to `regexp`. | .* |
| sender-domain <domain_str> | Enter the domain part of sender email address to define sender (`MAIL FROM:`) email addresses that match this policy. | |
| sender-name <local-part_str> | Enter the local part of sender email address to define sender (`MAIL FROM:`) email addresses that match this policy. | |
| sender-type {email-address-group \| ldap-group \| regexp \| user} | Enter one of the following ways to define sender (`MAIL FROM:`) email addresses that match this policy.<br>If you enter `ldap-group`, also configure `profile-ldap profile-ldap` by entering an LDAP profile in which you have enabled and configured a group query. | user |
| 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.<br>Disable to require that the sender email address in the SMTP envelope match the authenticated user name.<br>This option 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.<br>This option 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.<br>This option is applicable only if `smtp auth` is used. | |
| status {enable \| disable} | Enable to apply this policy. | enable |

## Related topics

ms365 profile antivirus on page 151

policy access-control delivery on page 157

config policy delivery-control on page 159

# profile access-control

Use this command to configure access control rules.

Note that all access control rules operate at the system level. Only system level profiles (for example, email groups) can be used by access control rules.

## Syntax

```
config profile access-control
   edit <profile_name>
      config access-control
         edit <id>
            set action {discard | receive | reject | relay | safe | safe-relay}
            set authenticated {any | authenticated | not-authenticated}
            set recipient-pattern <string>
            set recipient-pattern-ldap-groupname <group_name>
            set recipient-pattern-ldap-profile <profile_name>
            set recipient-pattern-group <group_name>
            set recipient-pattern-type {default | external | group | internal | ldap
                 | ldap-query | regexp}
            set reverse-dns-pattern <string>
            set reverse-dns-pattern-regexp {yes | no}
            set sender-ip-mask <ipv4mask>
            set sender-ip-type {geoip-group | ip-group | ip-mask}
            set sender-pattern <string>
            set sender-pattern-group <group_name>
            set sender-pattern-ldap-groupname <group_name>
            set sender-pattern-ldap-profile <profile_name>
            set sender-pattern-type {default | external | group | internal | ldap |
                 ldap-query | regexp}
            set status {enable | disable}
            set tls-profile <profile_name>
      end
end
```

| Variable | Description | Default |
|---|---|---|
| action {discard \| receive \| reject \| relay \| safe \| safe-relay} | Enter an action for the profile:<br>• `discard`: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.<br>• `receive`: Enter to only accept incoming email to protected domains if it passes all configured scans.<br>• `reject`: Enter to reject the email and reply to the SMTP client with SMTP reply code 550. | reject |

| Variable | Description | Default |
|---|---|---|
| | • `relay`: Enter to relay or proxy, process, and deliver the email normally if it passes all configured scans.<br>**Note**: Do not apply greylisting.<br>• `safe`: Enter to relay or proxy and deliver the email only if the recipient belongs to a protected domain or the sender is authenticated.<br>All antispam profile processing will be skipped, but antivirus, content and other scans will still occur.<br>• `safe-relay`: Enter to relay or proxy and deliver the email.<br>All antispam profile processing will be skipped, but antivirus, content, and other scans will still occur. | |
| authenticated {any \| authenticated \| not-authenticated} | Enter whether or not to match this access control rule based on client authentication:<br>• `any`: Match or do not match this access control rule regardless of whether the client has authenticated with the FortiMail unit.<br>• `authenticated`: Match this access control rule only for clients that have authenticated with the FortiMail unit.<br>• `not-authenticated`: Match this access control rule only for clients that have not authenticated with the FortiMail unit. | any |
| recipient-pattern <string> | Enter a pattern that defines recipient email addresses which match this rule, surrounded in slashes and single quotes (such as \'*\' ). | * |
| recipient-pattern-ldap-groupname <group_name> | Enter the LDAP group name to specify the recipient pattern.<br>This option is only available when `recipient-pattern-type` is set to `ldap`. | |
| recipient-pattern-ldap-profile <profile_name> | Enter the LDAP profile name to specify the recipient pattern.<br>This option is only available when `recipient-pattern-type` is set to either `ldap` or `ldap-query`. | |
| recipient-pattern-group <group_name> | Enter the group name to specify the recipient pattern.<br>This option is only available when `recipient-pattern-type` is set to `group`. | |
| recipient-pattern-type {default \| external \| group \| internal \| ldap \| ldap-query \| regexp} | Enter the pattern type:<br>• `default`: This is the user defined pattern. Also configure recipient-pattern <string>.<br>• `external`: Set for external recipients.<br>• `group`: If you enter this option, configure recipient-pattern-group <group_name>.<br>• `internal`: Set for internal recipients.<br>• `ldap`: If you enter this option, configure recipient-pattern-ldap-groupname <group_name> and recipient-pattern-ldap-profile <profile_name>.<br>• `ldap-query`: If you enter this option, configure recipient-pattern-ldap-profile <profile_name>.<br>• `regexp`: Use regular expression syntax instead of wildcards for the pattern. | default |
| reverse-dns-pattern <string> | Enter a pattern to compare to the result of a reverse DNS look-up of the IP address of the SMTP client delivering the email message. | * |

| Variable | Description | Default |
|---|---|---|
| | Because domain names in the SMTP session are self-reported by the connecting SMTP server and easy to fake, the FortiMail unit does not trust the domain name that an SMTP server reports. Instead, the FortiMail does a DNS lookup using the SMTP server's IP address. The resulting domain name is compared to the reverse DNS pattern for a match. If the reverse DNS query fails, the access control rule match will also fail. If no other access control rule matches, the connection will be rejected with SMTP reply code 550 (`Relaying denied`).<br>Wildcard characters allow you to enter partial patterns that can match multiple reverse DNS lookup results. An asterisk (*) represents one or more characters; a question mark (?) represents any single character.<br>For example, the recipient pattern `mail*.com` will match messages delivered by an SMTP server whose domain name starts with "mail" and ends with ".com".<br>**Note**: Reverse DNS queries for access control rules require that the domain name be a valid top level domain (TLD). For example, ".lab" is not a valid top level domain name, and thus the FortiMail unit cannot successfully perform a reverse DNS query for it. | |
| reverse-dns-pattern-regexp {yes \| no} | Enter `yes` to use regular expression syntax instead of wildcards to specify the reverse DNS pattern. | no |
| sender-ip-mask <ipv4mask> | Enter the sender's IP address. | 0.0.0.0/0 |
| sender-ip-type {geoip-group \| ip-group \| ip-mask} | Select the method of the SMTP client attempting to deliver the email message. | ip-mask |
| sender-pattern <string> | Enter a pattern that defines sender email addresses which match this rule, surrounded in slashes and single quotes (such as `\'*@example.com\'` ). | |
| sender-pattern-group <group_name> | Enter the group name to specify the sender pattern.<br>This option is only available when `sender-pattern-type` is set to `group`. | |
| sender-pattern-ldap-groupname <group_name> | Enter the LDAP group name to specify the sender pattern.<br>This option is only available when `sender-pattern-type` is set to `ldap`. | |
| sender-pattern-ldap-profile <profile_name> | Enter the LDAP profile name to specify the sender pattern.<br>This option is only available when `sender-pattern-type` is set to either `ldap` or `ldap-query`. | |
| sender-pattern-type {default \| external \| group \| internal \| ldap \| ldap-query \| regexp} | Enter the pattern type:<br>• `default`: This is the user defined pattern. Also configure sender-pattern <string>.<br>• `external`: Set for external senders.<br>• `group`: If you enter this option, configure sender-pattern-group <group_name>.<br>• `internal`: Set for internal senders.<br>• `ldap`: If you enter this option, configure sender-pattern-ldap-groupname <group_ | default |

| Variable | Description | Default |
|---|---|---|
| | name> and sender-pattern-ldap-profile <profile_name>.<br>• ldap-query: If you enter this option, configure sender-pattern-ldap-profile <profile_name>.<br>• regexp: Use regular expression syntax instead of wildcards for the pattern. | |
| status {enable \| disable} | Enable or disable the access control rule. | enable |
| tls-profile <profile_name> | Enter a TLS profile to allow or reject the connection based on whether the communication session attributes match the settings in the TLS profile.<br>If the attributes match, the access control action is executed.<br>If the attributes do **not** match, the FortiMail unit performs the ***Failure*** action configured in the TLS profile.<br>For more information on TLS profiles, see the FortiMail Administration Guide. | |

# profile antispam

Use this command to configure system-wide antispam profiles.

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

## Syntax

```
config profile antispam
   edit <profile_name> on page 171
      config bannedwords
         edit <word_str> on page 171
         set subject {enable | disable} on page 171
         set body {enable | disable} on page 172
      config dnsbl-server
         edit <server_name> on page 172
      config safelistwords
         edit <word_str> on page 172
            set subject {enable | disable} on page 172
            set body {enable | disable} on page 172
      config surbl-server
         edit <server_name> on page 172
      set action-banned-word <action_profile> on page 172
      set action-bayesian <action-profile_name> on page 172
      set action-behavior-analysis <action-profile_name> on page 172
      set action-bec <action-profile-name>
      set action-deep-header <action-profile_name> on page 172
      set action-default <action-profile_name> on page 172
      set action-dictionary <action-profile_name> on page 172
      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 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 action-fortiguard <action-profile_name> on page 173
set action-fortiguard-blockip <action-profile-name> on page 173
set action-fortiguard-phishing-uri <action-profile-name> on page 173
set action-grey-list <action-profile_name> on page 173
set action-heuristic <action-profile_name> on page 173
set action-image-spam <action-profile_name> on page 174
set action-impersonation-analysis <action> on page 173
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 action-newsletter <action-profile_name> on page 174
set action-rbl <action-profile_name> on page 174
set action-spf-fail <action> on page 174
set action-spf-neutral <action> on page 174
set action-spf-none <action> on page 174
set action-spf-pass <action> on page 174
set action-spf-perm-error <action> on page 174
set action-spf-sender-alignment <action> on page 174
set action-spf-soft-fail <action> on page 174
set action-spf-temp-error <action> on page 174
set action-surbl <action-profile_name> on page 175
set action-suspicious-newsletter <action-profile_name> on page 175
set action-uri-filter <action-profile_name> on page 175
set action-uri-filter-secondary <action-profile_name> on page 175
set action-virus <action-profile_name> on page 175
set aggressive {enable | disable} on page 175
set apply-action-default {enable | disable} on page 175
set banned-word {enable | disable} on page 175
set bayesian {enable | disable} on page 175
set behavior-analysis {enable | disable} on page 175
set bayesian-autotraining {enable | disable} on page 175
set bayesian-user-db {enable | disable} on page 175
set bayesian-usertraining {enable | disable} on page 175
set behavior-analysis {enable | disable}
set bec-profile <domain_name>
set bec-status {enable | disable}
set cousin-domain {enable | disable}
set cousin-domain-profile <domain_name>
set cousin-domain-scan-option {auto-detection body-detection header-
    detection}
set deepheader-analysis {enable | disable} on page 176
set deepheader-check-ip {enable | disable} on page 176
set dict-score <score_int> on page 176
set dictionary {enable | disable} on page 176
set dictionary-profile on page 176
set dictionary-type on page 176
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 dmarc-checking {enable | disable} on page 177
        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 dnsbl {enable | disable} on page 177
        set fortiguard-antispam {enable | disable} on page 177
        set fortiguard-check-ip {enable | disable} on page 177
        set fortiguard-phishing-uri {enable | disable} on page 177
        set greylist {enable | disable} on page 178
        set heuristic {enable | disable} on page 178
        set heuristic-lower <threshold_int> on page 178
        set heuristic-rules-percent <percentage_int> on page 178
        set heuristic-upper {threshold_int} on page 178
        set image-spam {enable | disable} on page 178
        set impersonation <profile_name> on page 178
        set impersonation-analysis {enable | disable} on page 178
        set impersonation-status {enable | disable}
        set ip-reputation-level1-status {enable | disable} on page 178
        set ip-reputation-level2-status {enable | disable} on page 178
        set ip-reputation-level3-status {enable | disable} on page 178
        set newsletter-status {enable | disable} on page 179
        set scan-bypass-on-auth {enable | disable} on page 179
        set scan-max-size <bytes_int> on page 179
        set scan-pdf {enable | disable} on page 180
        set spam-outbreak-protection {enable | disable | monitor-only} on page 180
        set spf-checking {enable | disable} on page 180
        set spf-fail-status {enable | disable} on page 179
        set spf-neutral-status {enable | disable} on page 179
        set spf-none-status {enable | disable} on page 179
        set spf-pass-status {enable | disable} on page 179
        set spf-sender-alignment-status {enable | disable}
        set spf-perm-error-status {enable | disable} on page 179
        set spf-soft-fail-status {enable | disable} on page 179
        set spf-temp-error-status {enable | disable} on page 179
        set surbl {enable | disable} on page 180
        set suspicious-newsletter-status {enable | disable} on page 180
        set uri-filter <filter> on page 180
        set uri-filter-secondary <filter> on page 180
        set uri-filter-secondary-status {enable | disable} on page 180
        set uri-filter-status {enable | disable} on page 181
        set virus {enable | disable} on page 181
        set safelist-enable {enable | disable} on page 181
        set safelist-word {enable | disable} on page 181
end
```

| Variable | Description | Default |
|---|---|---|
| <profile_name> | Enter the name of an antispam profile. | |
| <word_str> | Enter the banned word. You can use wildcards in banned words. But regular expressions are not supported. For more information about wildcards and regular expressions, see the FortiMail Administration Guide. | |
| subject {enable \| disable} | Enable to check the subject line for the banned word. | disable |

| Variable | Description | Default |
|---|---|---|
| body {enable \| disable} | Enable to check the message body for the banned word. | disable |
| <server_name> | Enter a DNSBL server name to perform a DNSBL scan. The FortiMail unit will query DNS blocklist servers. | |
| <server_name> | Enter a SURBL server name to perform a SURBL scan. The FortiMail unit will query SURBL servers. | |
| <word_str> | Enter the safelisted word to configure. | |
| subject {enable \| disable} | Enable to check the subject line for the safelisted word. | disable |
| body {enable \| disable} | Enable to check the message body for the safelisted word. | disable |
| action-banned-word <action_profile> | Enter the action profile that you want the FortiMail unit to use if the banned word scan determines that the email is spam. | |
| action-bayesian <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the Bayesian scan determines that the email is spam. | |
| action-behavior-analysis <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the behavior analysis scan determines that the email is spam. | |
| action-bec <action-profile-name> | Enter the action profile that you want the FortiMail unit to use if the BEC check determines that the email is spam. | |
| action-deep-header <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the deep header scan determines that the email is spam. | |
| action-default <action-profile_name> | Enter the default action profile that you want all scanners of the FortiMail unit to use. However, if you choose an action profile other than “default" for a scanner, this scanner will use the chosen profile. | |
| action-dictionary <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the heuristic scan determines that the email is spam. | |
| action-dkim-fail <action-profile_name> | Enter the action profile that you want the FortiMail unit to use for DKIM check failure. | |
| action-dkim-none <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if no DKIM DNS record is not found or parsed correctly. | |

| Variable | Description | Default |
|---|---|---|
| action-dkim-pass <action-profile_name> | Enter the action profile that you want the FortiMail unit to use for DKIM check pass. | |
| action-dkim-temp-error <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if DNS server returns Temp error when querying the DKIM DNS record. | |
| action-dmarc-fail <action-profile_name> | Enter the action profile that you want the FortiMail unit to use for DMARC check failure. | |
| action-dmarc-none <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if no DMARC DNS record is not found or parsed correctly. | |
| action-dmarc-pass <action-profile_name> | Enter the action profile that you want the FortiMail unit to use for DMARC check pass. | |
| action-dmarc-temp-error <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if DNS server returns Temp error when querying the DMARC DNS record. | |
| action-fortiguard <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the FortiGuard Antispam scan determines that the email is spam. | |
| action-fortiguard-blockip <action-profile-name> | Enter the action profile that you want the FortiMail unit to use if the FortiGuard block IP scan determines that the email is spam. | |
| action-fortiguard-phishing-uri <action-profile-name> | Enter the action profile that you want the FortiMail unit to use if the FortiGuard phishing URI scan determines that the email is spam. | |
| action-grey-list <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the grey list scan determines that the email is spam. | |
| action-heuristic <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the heuristic scan determines that the email is spam. | |
| action-impersonation-analysis <action> | Enter the action profile that you want the FortiMail unit to use if the impersonation alaysis determines the email is from someone impersonating a known email address. | |

| Variable | Description | Default |
|---|---|---|
| action-image-spam <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the image scan determines that the email is spam. | |
| action-ip-reputation-level1 <action-profile_name> | Enter the action profile that you want assigned to IP reputation level 1. See set ip-reputation-level1-status {enable \| disable} on page 178 for more information.<br>FortiGuard categorizes the blocklisted IP addresses into three levels, level 1 has the worst reputation and level 3 the best. | |
| action-ip-reputation-level2 <action-profile_name> | Enter the action profile that you want assigned to IP reputation level 2. See set ip-reputation-level2-status {enable \| disable} on page 178 for more information.<br>FortiGuard categorizes the blocklisted IP addresses into three levels, level 1 has the worst reputation and level 3 the best. | |
| action-ip-reputation-level3 <action-profile_name> | Enter the action profile that you want assigned to IP reputation level 3. See set ip-reputation-level3-status {enable \| disable} on page 178 for more information.<br>FortiGuard categorizes the blocklisted IP addresses into three levels, level 1 has the worst reputation and level 3 the best. | |
| action-newsletter <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the newsletter scan determines that the email is spam. | |
| action-rbl <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the RBL scan determines that the email is spam. | |
| action-spf-fail <action> | Enter the action FortiMail performs if the SPF fails, which means the host is not authorized to send messages. | |
| action-spf-neutral <action> | Enter the action FortiMail performs if SPF neutral fails, which means the SPF record is found but no definitive assertion. | |
| action-spf-none <action> | Enter the action FortiMail performs if SPF none fails, whichs means there is no SPF record. | |
| action-spf-pass <action> | Enter the action FortiMail performs if SPF pass fails, which means it discovers the host is not authorized to send a message. | |
| action-spf-perm-error <action> | Enter the action FortiMail performs if SPF perm error fails, which means the SPF records are invalid. | |
| action-spf-sender-alignment <action> | Enter the action FortiMail performs if SPF sender alignment fails, which means the header from the subject authorization domain mismatch. | |
| action-spf-soft-fail <action> | Enter the action Fortimail takes if spf soft fail fails, which means the host is not authorized to send messages but not a strong statement. | |
| action-spf-temp-error <action> | Enter the action FortiMail performs if action SPF temp error fails, which means there is a processing error. | |

| Variable | Description | Default |
|---|---|---|
| action-surbl <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the SURBL scan determines that the email is spam. | |
| action-suspicious-newsletter <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the suspicious newsletter scan determines that the email is spam. | |
| action-uri-filter <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the URI filter scan determines that the email is spam. | |
| action-uri-filter-secondary <action-profile_name> | Enter the action profile that you want the FortiMail unit to use if the URI filter scan determines that the email is spam. | |
| action-virus <action-profile_name> | Enter the action profile that requires the FortiMail unit to treat messages with viruses as spam. | |
| aggressive {enable \| disable} | Enable this option to examine file attachments in addition to embedded images.<br>To improve performance, enable this option only if you do not have a satisfactory spam detection rate. | disable |
| apply-action-default {enable \| disable} | Enable this option to apply default action to all messages. | disable |
| banned-word {enable \| disable} | Enable this option to scan banned words for this antispam profile. | disable |
| bayesian {enable \| disable} | Enable this option to activate Bayesian scan for this antispam profile. | disable |
| behavior-analysis {enable \| disable} | Enable this option to activate behavior analysis scan for this antispam profile. | disable |
| bayesian-autotraining {enable \| disable} | Enable to use FortiGuard Antispam and SURBL scan results to train per-user Bayesian databases that are not yet mature (that is, they have not yet been trained with 200 legitimate email and 100 spam in order to recognize spam). | enable |
| bayesian-user-db {enable \| disable} | Enable to use per-user Bayesian databases.<br>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 |
|---|---|---|
| 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.<br>See also antispam behavior-analysis on page 42 to adjust the BA aggressiveness level. | disable |
| bec-profile <domain_name> | Enter the BEC profile used by this profile to prevent spam attacks. | |
| bec-status {enable \| disable} | Enable the business email compromise (BEC) check. | |
| cousin-domain {enable \| disable} | **Note:** For this subcommand to take effect, `impersonation-status` must be set to `enable`.<br>Enable the cousin domain feature to mitigate business email compromise (BEC) email-impersonation risks due to domain names being deliberately misspelled. | disable |
| cousin-domain-profile <domain_name> | Enter the cousin domain profile used by this profile to prevent domain name impersonation. | |
| cousin-domain-scan-option {auto-detection body-detection header-detection} | Enter cousin domain scan options for detecting misspelled domain names either automatically, within the email body, and/or the email header.<br>Separate each option with a space for multiple scan options. | header-detection body-detection auto-detection |
| deepheader-analysis {enable \| disable} | Enable to inspect all message headers for known spam characteristics.<br>If the FortiGuard Antispam scan is enabled, this option uses results from that scan, providing up-to-date header analysis. For more information, see "set as profile modify fortishield" on page 184. | disable |
| deepheader-check-ip {enable \| disable} | Enable to query for the blocklist status of the IP addresses of all SMTP servers appearing in the `Received:` lines of header lines.<br>If this option is disabled, the FortiMail unit checks only the IP address of the current SMTP client.<br>This option applies only if you have also configured either or both FortiGuard Antispam scan and DNSBL scan. For more information, see "set as profile modify fortishield" on page 184 and "set as profile modify dnsbl" on page 181. | disable |
| dict-score <score_int> | Enter the number of dictionary term matches above which the email will be considered to be spam. | |
| dictionary {enable \| disable} | Enable to perform a dictionary scan for this profile. | disable |
| dictionary-profile | Enter the dictionary profile name. | |
| dictionary-type | Enter the type of dictionary profile. | |
| dkim-checking {enable \| disable} | Enable to have the unit perform email authentication with DKIM checking. If either SPF check or DKIM check passes, DMARC check will pass. If both fail, DMARC fails. | disable |

| Variable | Description | Default |
|---|---|---|
| dkim-fail-status {enable \| disable} | Enable or disable checking invalid DKIM body hash or signature. | enable |
| dkim-none-status {enable \| disable} | Enable or disable checking for instances where no DKIM DNS record is found, 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 Temp 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-pass-status {enable \| disable} | Enable or disable DMARC check passing. | 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. | disable |
| dnsbl {enable \| disable} | Enable to perform a DNSBL scan for this profile. The FortiMail unit will query DNS blocklist servers defined using “set out_profile profile modify deepheader" on page 405. | disable |
| fortiguard-antispam {enable \| disable} | Enable to let the FortiMail unit query the FortiGuard Antispam service to determine if any of the uniform resource identifiers (URI) in the message body are associated with spam. If any URI is 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 include whether or not the IP address of the SMTP client is blocklisted in the FortiGuard Antispam query. | disable |
| fortiguard-phishing-uri {enable \| disable} | Enable to include whether or not the phishing URI 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_int> | Enter the score equal to or below which the FortiMail unit considers an email to **not** be spam. | -20.000000 |
| heuristic-rules-percent <percentage_int> | Enter the percentage of the total number of heuristic rules that will be used to calculate the heuristic score for an email message.<br>The FortiMail unit compares this total score to the upper and lower level threshold to determine if an email is:<br>• spam<br>• not spam<br>• indeterminable (score is between the upper and lower level thresholds)<br>To improve system performance and resource efficiency, enter the lowest percentage of heuristic rules that results in a satisfactory spam detection rate. | 100 |
| heuristic-upper {threshold_int} | Enter the score equal to or above which the FortiMail unit considers an email to be spam. | 10.000000 |
| image-spam {enable \| disable} | Enable to perform an image spam scan. | disable |
| impersonation <profile_name> | Enter the impersonation profile used by this profile to prevent email spoofing attacks. | |
| impersonation-analysis {enable \| disable} | **Note:** For this subcommand to take effect, `impersonation-status` must be set to `enable`.<br>Enable sender impersonation analysis to automatically learn and track the mapping of display names and internal email addresses to prevent spoofing attacks. | disable |
| impersonation-status {enable \| disable} | Enable the sender impersonation feature.<br>Once enabled, `cousin-domain`, `impersonation-analysis`, and `spf-sender-alignment-status` can take effect. | disable |
| ip-reputation-level1-status {enable \| disable} | Enable IP reputation to enable the FortiMail unit to query the FortiGuard Antispam service to determine if the public IP address of the SMTP client is blocklisted.<br>FortiGuard categorizes the blocklisted IP addresses into three levels, level 1 has the worst reputation and level 3 the best. | disable |
| ip-reputation-level2-status {enable \| disable} | Enable IP reputation to enable the FortiMail unit to query the FortiGuard Antispam service to determine if the public IP address of the SMTP client is blocklisted.<br>FortiGuard categorizes the blocklisted IP addresses into three levels, level 1 has the worst reputation and level 3 the best. | disable |
| ip-reputation-level3-status {enable \| disable} | Enable IP reputation to enable the FortiMail unit to query the FortiGuard Antispam service to determine if the public IP address of the SMTP client is blocklisted.<br>FortiGuard categorizes the blocklisted IP addresses into three levels, level 1 has the worst reputation and level 3 the best. | disable |

| Variable | Description | Default |
|---|---|---|
| newsletter-status {enable \| disable} | Enable dection of newsletters to make sure newsletters and other marketing campaigns are not spam. | |
| spf-fail-status {enable \| disable} | Enable to make the FortiMail unit check if the host is not authorized to send messages.<br>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.<br>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.<br>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.<br>If the client IP address fails the SPF check, FortiMail takes the antispam action configured in action-spf-pass. | |
| spf-sender-alignment-status {enable \| disable} | **Note:** For this subcommand to take effect, `impersonation-status` must be set to `enable`.<br>Enable to make the FortiMail unit check if the header from the authorization domain is mismatched.<br>If the client IP address fails the SPF check, FortiMail takes the desired action entered in action-spf-sender-alignment. | |
| spf-perm-error-status {enable \| disable} | Enable to make the FortiMail unit check if the SPF records are invalid.<br>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.<br>If the client IP address fails the SPF check, FortiMail takes the antispam action entered in action-spf-soft-fail. | |
| spf-temp-error-status {enable \| disable} | Enable to make the FortiMail unit check if there is a processing error.<br>If the client IP address fails the SPF check, FortiMail takes the antispam action entered in `action-spf-temp-error`. | |
| 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.<br>To scan all email regardless of size, enter `0`. | 1204 bytes for predefined profiles |

| Variable | Description | Default |
|---|---|---|
| | | 600 bytes 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 |
| spam-outbreak-protection {enable \| disable \| monitor-only} | Enable to temporarily hold suspicious email for a certain period of time (configurable with `outbreak-protection-period` under config system fortiguard antispam on page 280) if the enabled FortiGuard antispam check (block IP and/or URI filter) returns no result. After the specified time interval, FortiMail will query the FortiGuard server for the second time. This provides an opportunity for the FortiGuard antispam service to update its database in cases a spam outbreak occurs.<br>When set to `monitor-only`, email is not deferred. Instead, "X-FEAS-Spam-outbreak: monitor-only" is inserted as its header, 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 246.<br>Starting from 6.0.3 release, you can also specify different actions toward defferent SPS check results:<br>• **spf-fail-status**: the host is not authorized to send messages.<br>• **spf-soft-fail-status**: the host is not authorized to send messages but not a strong statement.<br>• **spf-sender-alighnment-status**: Header From and autorization domain mismatch.<br>• **spf-perm-error-status**: the SPF records are invalid.<br>• **spf-temp-error-status**: Temporary proccessing error.<br>• **spf-pass-status**: the host is authorized to send messages.<br>• **spf-neutral-status**: SPF record is found but no definitive assertion.<br>• **spf-none-status**: No SPF record. | disable |
| surbl {enable \| disable} | Enable to perform a SURBL scan. The FortiMail unit will query SURBL servers defined using "set out_profile profile modify surblserver" on page 421. | disable |
| suspicious-newsletter-status {enable \| disable} | Enable the detection of newsletters. | disable |
| uri-filter <filter> | Specify the URI filter to use. | |
| uri-filter-secondary <filter> | To take different actions towards different URI filters/categories, you can specify a primary and a secondary filter, and specify different actions for each filter. If both URI filters match an email message, the primary filter action will take precedence. | |
| uri-filter-secondary-status {enable \| disable} | Enable or disable the secondaryURI filter scan. | disable |

| Variable | Description | Default |
|---|---|---|
| uri-filter-status {enable \| disable} | Enable or disable URI filter scan. | disable |
| virus {enable \| disable} | Enable to treat email with viruses as spam. When enabled, instead of performing the action configured in the antivirus profile, the FortiMail unit will instead perform either the general or individualized action in the antispam profile. For details, see “set out_profile profile modify individualaction" on page 415 and “set out_profile profile modify actions" on page 400. | disable |
| 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. The scan will examine the email for words configured in “set out_profile profile modify safelistwordlist" on page 426. | disable |

## Related topics

profile antispam-action on page 181
profile antivirus on page 185

# profile antispam-action

Use this command to configure antispam action profiles.

## Syntax

```
config profile antispam-action
   edit <profile_name> on page 182
      set action {discard | domain-quarantine | none | personal-quarantine |
           reject | rewrite-rcpt | system-quarantine} on page 182
      set alternate-host {<relay_fqdn> | <relay_ipv4>} on page 182
      set alternate-host-status {enable | disable} on page 182
      set archive-account <account_name> on page 182
      set archive-status {enable | disable} on page 183
      set bcc-addr <recipient_email> on page 183
      set bcc-env-from-addr <message_str>
      set bcc-env-from-status {enable | disable}
      set bcc-status {enable | disable} on page 183
      set deliver-to-original-host {enable | disable} on page 183
      set disclaimer-insertion {enable | disable} on page 183
      set disclaimer-insertion-content <message_name> on page 183
      set disclaimer-insertion-location {beginning | end} on page 183
      set header-insertion-name <name_str> on page 183
      set header-insertion-status {enable | disable} on page 183
      set header-insertion-value <header_str> on page 183
      set notification-profile <profile_name> on page 184
      set notification-status {enable | disable} on page 184
      set rewrite-rcpt-local-type {none | prefix | replace | suffix} on page 184
```

```
        set rewrite-rcpt-local-value <value_str> on page 184
        set rewrite-rcpt-domain-type {none-prefix | replace | suffix} on page 184
        set rewrite-rcpt-domain-value <value_str> on page 184
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.<br>• `discard`: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.<br>• `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.<br>• `none`: Apply any configured header or subject line tags, if any.<br>• `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.<br>• `reject`: Enter to reject the email and reply to the SMTP client with SMTP reply code 550.<br>• `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).<br>If you enter this option, also configure rewrite-rcpt-local-type {none \| prefix \| replace \| suffix} on page 184, rewrite-rcpt-local-value <value_str> on page 184, rewrite-rcpt-domain-type {none-prefix \| replace \| suffix} on page 184, and rewrite-rcpt-domain-value <value_str> on page 184.<br>• `system-quarantine`: Enter to redirect spam to the system quarantine. For more information, see the FortiMail Administration Guide. | none |
| alternate-host {<relay_fqdn> \| <relay_ipv4>} | Type the fully qualified domain name (FQDN) or IP address of the alternate relay or SMTP server.<br>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>} on page 182.<br>**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 on page 137 and the protected domain's tp-use-domain-mta {yes \| no} on page 114. | disable |
| archive-account <account_name> | Type the email archive account name where you want to archive the spam.<br>Enable archive-status {enable \| disable} on page 183 to make this function work.<br>For more information about archive accounts, see antispam url-fgas-exempt-list on page 56. | |

| Variable | Description | Default |
|---|---|---|
| archive-status {enable \| disable} | Enable to allow the archive-account <account_name> on page 182 function to work. | disable |
| bcc-addr <recipient_ email> | Type the blind carbon copy (BCC) recipient email address.<br>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.<br>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> on page 183. | 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 |
| 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.<br>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.<br>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:<br>`X-Custom-Header: Detected as spam by profile 22.`<br>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.<br>**Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.<br>See header-insertion-value <header_str> on page 183. | |
| header-insertion-status {enable \| disable} | Enable to add a message header to detected spam.<br>See header-insertion-value <header_str> on page 183. | disable |
| header-insertion-value <header_str> | Enter the message header value. | |

| Variable | Description | Default |
|---|---|---|
| | Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:<br>`X-Custom-Header: Detected as spam by profile 22.`<br>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.<br>**Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.<br>See header-insertion-name <name_str> on page 183. | |
| 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 |
| 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.<br>`none`: No change.<br>`prefix`: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str> on page 184.<br>`suffix`: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str> on page 184.<br>`replace`: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str> on page 184. | 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} on page 184. | |
| 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.<br>`none`: No change.<br>`prefix`: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <value_str> on page 184.<br>`suffix`: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <value_str> on page 184.<br>`replace`: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <value_str> on page 184. | 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} on page 184. | |

## Related topics

profile antispam on page 169

# 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> on page 185
    set action-default { predefined_av_discard | predefined_av_reject} on page
        185
    set action-file-signature on page 185
    set action-heuristic {predefined_av_discard | predefined_av_reject} on page
        186
    set action-outbreak <action> on page 186
    set action-sandbox-high <action> on page 186
    set action-sandbox-low <action> on page 186
    set action-sandbox-medium <action> on page 186
    set action-sandbox-noresult <action>
    set action-sandbox-uri-high <action> on page 186
    set action-sandbox-uri-low <action> on page 186
    set action-sandbox-uri-medium <action> on page 186
    set action-sandbox-uri-noresult <action>
    set action-sandbox-uri-virus <action> on page 186
    set action-sandbox-virus <action> on page 186
    set file-signature-check {enable | disable} on page 186
    set grayware-scan {enable | disable} on page 186
    set heuristic {enable | disable} on page 186
    set malware-outbreak-protection {enable | disable} on page 186
    set sandbox-analysis {enable | disable} on page 187
    set sandbox-analysis-uri{enable | disable} on page 187
    set sandbox-scan-mode {submit-and-wait | submit-only} on page 187
    set scanner {enable | disable} on page 187
end
```

| Variable | Description | Default |
|---|---|---|
| <profile_name> | Enter the name of the profile.<br>To view a list of existing entries, enter a question mark ( ? ). | |
| action-default { predefined_av_ discard \| predefined_ av_reject} | Type a predefined antivirus action.<br>predefined_av_discard: Accept infected email, but then delete it instead of delivering the email, without notifying the SMTP client.<br>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 file signature action.<br>predefined_av_discard:<br>predefined_av_reject: | |

| Variable | Description | Default |
|---|---|---|
| action-heuristic {predefined_av_discard \| predefined_av_reject} | Type a predefined heuristic scanning action on infected email.<br>`predefined_av_discard`: Accept email suspected to be infected, but then delete it instead of delivering the email, without notifying the SMTP client.<br>`predefined_av_reject`: Reject email suspected to be infected, and reply to the SMTP client with SMTP reply code 550. | |
| 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-uri-high <action> | Type to determine the action to take if the FortiSandbox URI analysis determines that the email messages have high probability of viruses or other threat qualities. | default |
| action-sandbox-uri-low <action> | Type to determine the action to take if the FortiSandbox URI analysis determines that the email messages have low probability of viruses or other threat qualities. | default |
| action-sandbox-uri-medium <action> | Type to determine the action to take if the FortiSandbox URI determines that the email messages have medium probability of viruses or other threat qualities. | default |
| action-sandbox-uri-virus <action> | Type to determine the action to take if the FortiSandbox URI analysis determines that the email messages definitely have viruses or other threat qualities. | default |
| action-sandbox-uri-noresult <action> | Type to determine the action to take if the FortiSandbox URI 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 |
| 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. | |

| Variable | Description | Default |
|---|---|---|
| | This feature can help quickly identify new threats.<br>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 284. | disable |
| sandbox-analysis-uri {enable \| disable} | Enable or disable sending suspicious attachment content to FortiSandbox for analysis. | disable |
| sandbox-scan-mode {submit-and-wait \| submit-only} | Edits 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

profile antispam on page 169

# profile antivirus-action

Use this command to configure antivirus action profiles.

## Syntax

```
config profile antivirus-action
   edit <profile_name> on page 182
      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 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.<br>• `discard`: Enter to accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.<br>• `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.<br>• `none`: Apply any configured header or subject line tags, if any.<br>• `reject`: Enter to reject the email and reply to the SMTP client with SMTP reply code 550.<br>• `repackage`: Forward the infected email as an attachment but the original email body will still be used without modification.<br>• `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”.<br>• `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).<br>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>.<br>• `system-quarantine`: Enter to redirect virus to the system quarantine. For more information, see the FortiMail Administration Guide. | none |
| alternate-host {<relay_fqdn> \| <relay_ipv4>} | Type the fully qualified domain name (FQDN) or IP address of the alternate relay or SMTP server.<br>This field applies only if `alternate-host-status` is `enable`. | |

| Variable | Description | Default |
|---|---|---|
| alternate-host-status {enable \| disable} | Enable to route the email to a specific SMTP server or relay. Also configure alternate-host {<relay_fqdn> \| <relay_ipv4>}.<br>**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 on page 137 and the protected domain's tp-use-domain-mta {yes \| no} on page 114. | 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.<br>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.<br>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.<br>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.<br>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:<br>`X-Custom-Header: Detected as virus by profile 22.`<br>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.<br>**Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822. | |

| Variable | Description | Default |
|---|---|---|
| | See header-insertion-value <header_str>. | |
| header-insertion-status {enable \| disable} | Enable to add a message header to detected virus.<br>See header-insertion-value <header_str>. | disable |
| header-insertion-value <header_str> | Enter the message header value.<br>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:<br>`X-Custom-Header: Detected as virus by profile 22.`<br>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.<br>**Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.<br>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 |
| 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 |
| 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.<br>`none`: No change.<br>`prefix`: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str>.<br>`suffix`: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str>.<br>`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.<br>`none`: No change.<br>`prefix`: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <value_str>.<br>`suffix`: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. | none |

| Variable | Description | Default |
|---|---|---|
| | `replace`: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <value_str>. | |
| 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> on page 191 ("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 on page 185

# 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> on page 192
    set auth-type {auto | cram-md5 | digest-md5 | login | ntlm | plain}
```

```
        set option {ssl secure tls senddomain} on page 192
        set port <port_int> on page 193
        set server {<fqdn_str> | <host_ipv4>} on page 193
    config profile authentication pop3
      edit <profile_name> on page 192
        set auth-type {auto | cram-md5 | digest-md5 | login | ntlm | plain}
        set option {ssl secure tls senddomain} on page 193
        set port <port_int> on page 193
        set server {<fqdn_str> | <host_ipv4>} on page 193
    config profile authentication radius
      edit <profile_name> on page 192
        set access-override {enable | disable} on page 192
        set access-override-attribute <integer> on page 192
        set  access-override-vendor <integer> on page 192
        set auth-prot {auto | chap | mschap | mschap2 | pap} on page 193
        set domain-override {enable | disable} on page 193
        set domain-override-attribute <integer> on page 193
        set domain-override-vendor <integer> on page 193
        set nas-ip <ip_addr> on page 193
        set port <port_int> on page 193
        set secret <password_str> on page 193
        set send-domain {enable | disable} on page 194
        set server {<fqdn_str> | <host_ipv4>} on page 194
    config profile authentication smtp
      edit <profile_name> on page 192
        set auth-type {auto | cram-md5 | digest-md5 | login | ntlm | plain}
        set option {ssl secure tls senddomain} on page 194
        set server {<fqdn_str> | <host_ipv4>} on page 194
        set port <port_int> on page 194
        set try-ldap-mailhost {enable | disable} on page 194
end
```

| Variable | Description | Default |
|---|---|---|
| <profile_name> | Enter the name of the profile.<br>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:<br>• `senddomain`: Enable if the IMAP server requires both the user name and the domain when authenticating. | |

| Variable | Description | Default |
|---|---|---|
| | • `ssl`: Enables secure socket layers (SSL) to secure message transmission.<br>• `secure`: Enables secure authentication.<br>• `tls`: Enables transport layer security (TLS) to ensure privacy between communicating application. | |
| port <port_int> | Enter the TCP port number of the IMAP server.<br>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:<br>• `domain`: Enable if the POP3 server requires both the user name and the domain when authenticating.<br>• `ssl`: Enables secure socket layers (SSL) to secure message transmission.<br>• `secure`: Enables secure authentication.<br>• `tls`: Enables transport layer security (TLS) to ensure privacy between communicating application. | |
| port <port_int> | Enter the TCP port number of the POP3 server.<br>The standard port number for SSL-secured POP3 is 995. | 110 |
| 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. | |

| Variable | Description | Default |
|---|---|---|
| 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:<br>• `senddomain`: Enable if the SMTP server requires both the user name and the domain when authenticating.<br>• `ssl`: Enables secure socket layers (SSL) to secure message transmission.<br>• `secure`: Enables secure authentication.<br>• `tls`: Enables transport layer security (TLS) to ensure privacy between communicating application | |
| server {<fqdn_ str> \| <host_ ipv4>} | Enter the IP address or fully qualified domain name (FQDN) of the SMTP server. | |
| port <port_int> | Enter the TCP port number of the SMTP server.<br>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.<br>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 on page 196
profile encryption on page 212

# profile bec

Use this command to configure business email compromise (BEC) profile rules. To avoid false positives and false negatives, assign scores to adjust the weight allocated to each of the most common BEC attack types, such as cousin domains, suspicious characters, sender alignment, action keywords, and URL categories.

Once configured, BEC profiles are then used in antispam profiles.

## Syntax

```
config profile bec
   edit <name>
      config rule
      set comment <string>
         edit <order-integer>
```

```
            set action <datasource>
            set action-keyword-score <float>
            set cousin-domain-score <float>
            set malformed-email-score <float>
            set name <string>
            set sender-alignment-score <float>
            set status {enable | disable}
            set suspicious-character-score <float>
            set threshold <float>
            set url-profile <datasource>
            set url-profile-score <float>
        next
    end
end
```

| Variable | Description | Default |
|---|---|---|
| action <datasource> | Enter an antispam action profile name for the rule. | |
| action-keyword-score <float> | Enter a weight-adjusted score for actions keywords. | 10.000000 |
| cousin-domain-score <float> | Enter a weight-adjusted score for cousin domains. | 10.000000 |
| malformed-email-score <float> | Enter a weight-adjusted score for malformed emails.<br>Malformed emails are those emails that contain malformed data in the email structure, header, or body. For more information, see RFC 7103. | 10.000000 |
| name <string> | Enter a name for the rule. | |
| sender-alignment-score <float> | Enter a weight-adjusted score for sender alignment.<br>Sender alignment checks for a Header From and Envelope From domain mismatch. | 10.000000 |
| status {enable \| disable} | Enable or disable the profile rule. | enable |
| suspicious-character-score <float> | Enter a weight-adjusted score for suspicious characters. | 10.000000 |
| threshold <float> | Define the threshold at which point actions are taken. This score is allocated to the other categories. | 50.000000 |
| url-profile <datasource> | Enter a URL profile to assign to the URL category (`url-profile-score`). | unrated |
| url-profile-score <float> | Enter a weight-adjusted score for URL profiles that analyze any phishing URLs contained within emails. | 10.000000 |

## Related topics

profile antispam

# 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> on page 196
      set address-pattern <pattern_str> on page 196
      set key-private <key_str> on page 196
      set key-public <key_str> on page 196
      set key-usage {both | encryption | signing} on page 196
      set password <pwd_str> on page 196
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 on page 191

profile encryption on page 212

# 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> on page 198
    config attachment-scan
      edit <index_number>
        set action <action> on page 198
        set operator {is | is-not} on page 198
        set patterns {archive | audio | encrypted | executable_windows | image
            | msoffice | openoffice | script | video} on page 198
        set status {enable | disable} on page 198
    config monitor
      edit monitor <index_int> on page 198
        set action <profile_name> on page 198
        set dict-score <score_int> on page 198
        set dictionary-group <dictionary-group_name> on page 198
        set dictionary-profile <dictionary-profile_name> on page 199
        set dictionary-type {group | profile} on page 199
        set scan-msoffice {enable | disable} on page 199
        set scan-pdf {enable | disable} on page 199
        set status {enable | disable} on page 199
    set action-cdr <action_profile> on page 199
    set action-default <action_profile> on page 199
    set action-image-analysis <action_profile> on page 199
    set action-max-size <action-profile> on page 199
    set archive-scan-options {block-on-failure-to-decompress on page 199 | block-
        password-protected on page 199 | block-recursive on page 199}
    set cdr-file-type-options {msoffice | pdf} on page 200
    set decrypt-password-archive {enable |disable} on page 200
    set decrypt-password-num-of-words <number> on page 200
    set decrypt-password-office {enable | disable} on page 200
    set decrypt-password-options {built-in-password-list | user-defined-
        password-list | words-in-email-content} on page 200
    set defersize <size-in-kb> on page 200
    set embedded-scan-options {check-msoffice | check-msoffice-vba | check-
        msvisio | check-openoffice | check-pdf} on page 200
    set html-content-action {convert-to-text | modify-content} on page 200
    set html-content-uri-action {click-protection | click-protection-isolator |
        isolator | keep | remove}
    set html-content-uri-selection {tag-attribute | tag-content}
```

```
        set image-analysis-scan {enable | disable} on page 201
        set max-num-of-attachment <number> on page 201
        set max-size <size-in-kb> on page 201
        set max-size-option {message | attachment} on page 201
        set max-size-status {enable | disable} on page 201
        set remove-active-content {enable | disable}
        set scan options block-fragmented-email on page 201
        set scan options block-password-protected-office on page 201
        set scan options check-archive-content on page 201
        set scan options check-embedded-content on page 201
        set scan options bypass-on-smtp-auth on page 201
        set scan options check-html-content on page 201
        set scan options check-max-num-of-attachment on page 202
        set scan options check-text-content on page 202
        set scan options defer-message-delivery on page 202
        set text-content-action {remove-uri | click-protection} on page 202
end
```

| Variable | Description | Default |
|---|---|---|
| <profile_name> | Enter the name of the profile.<br>To view a list of existing entries, enter a question mark ( ? ). | |
| action <action> | Specify the action to use. | |
| operator {is \| is-not} | Specify the operator. | is |
| patterns {archive \| audio \| encrypted \| executable_ windows \| image \| msoffice \| openoffice \| script \| video} | Enter the pattern/s that match the email attachment names that you want the content profile to match.<br>For multiple patterns, separate each entry with a space. | |
| status {enable \| disable} | Enable or disable a pattern that matches the email attachment names that you want the content profile to match. | enable |
| monitor <index_ int> | Enter the index number of the monitor profile.<br>If the monitor profile does not currently exist, it will be created. | |
| action <profile_ name> | Enter the action profile for this monitor profile. The FortiMail unit will perform the actions if the content of the email message matches words or patterns from the dictionary profile that the monitor profile uses. | |
| dict-score <score_ 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 monitor profile will use.<br>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.<br>For information on dictionary profiles, see the FortiMail Administration Guide. | |

| Variable | Description | Default |
|---|---|---|
| dictionary-profile <dictionary-profile_name> | Enter the dictionary profile that this monitor profile will use.<br>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 203`.<br>For information on dictionary profiles, see the FortiMail Administration Guide. | |
| dictionary-type {group \| profile} | Enter `profile` to detect content based upon a dictionary profile, or `group` to detect content based upon a group of dictionary profiles. | group |
| scan-msoffice {enable \| disable} | Enable or disable MS Word document scanning for this profile. | disable |
| scan-pdf {enable \| disable} | Enable or disable PDF document scanning for this profile. | disable |
| status {enable \| disable} | Enable or disable this monitor profile. | disable |
| action-cdr <action_profile> | Specify the action profile to use. | |
| action-default <action_profile> | Enter a content action profile to be used by all the content filters except for the encrypted email, which can have its own action. See below for details. | |
| action-image-analysis <action_profile> | For the image email file type, you can use a content action profile to overwrite the default action profile used in the content profile. | |
| action-max-size <action-profile> | Specify the action profile to use for message over maximum size. | |
| block-on-failure-to-decompress | Enter to apply the action configured in profile content-action on page 203 if an attached archive cannot be successfully decompressed in order to scan its contents. | |
| block-password-protected | Enter to apply the action configured inprofile content-action on page 203 if an attached archive is password-protected. | |
| block-recursive | Enable to block archive attachments whose depth of nested archives exceeds `archive-max-recursive-level <depth_int> on page 199`. | |
| archive-max-recursive-level <depth_int> | Enter the nesting depth threshold. Depending upon each attached archive's depth of archives nested within the archive, the FortiMail unit will use one of the following methods to determine whether it should block or pass the email.<br>• The `archive-max-recursive-level` is `0`, or attachment's depth of nesting equals or is less than `archive-max-recursive-level`: If the attachment contains a file that matches one of the other MIME file types, perform the action configured for that file type, either block or pass.<br>• The attachment's depth of nesting is greater than `archive-max-recursive-level`: Apply the block action, unless you have disabled block-recursive on page 199, in which case it will pass the MIME file type content filter. Block actions are specified in the profile content-action on page 203. | 12 |

| Variable | Description | Default |
|---|---|---|
| cdr-file-type-options {msoffice \| pdf} | Specify the file type for content disarm and reconstruction. | |
| decrypt-password-archive {enable \|disable} | Enable or disable to decrypt password protected archives. | disable |
| decrypt-password-num-of-words <number> | Specify the number of words adjacent to the keyword to try for archive decryption. | 5 |
| decrypt-password-office {enable \| disable} | Enable to decrypt password protected Office files. | disable |
| decrypt-password-options {built-in-password-list \| user-defined-password-list \| words-in-email-content} | Specify which kind of password to use to decrypt the archives. | words-in-email-content |
| defersize <size-in-kb> | Bigger size will be deferred. 0 means no limit. | 0 |
| embedded-scan-options {check-msoffice \| check-msoffice-vba \| check-msvisio \| check-openoffice \| check-pdf} | 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.<br>Enable to, for MIME types such as Microsoft Office, Microsoft Visio, OpenOffice.org , and PDF documents, scan files that are encapsulated within the document itself. | |
| html-content-action {convert-to-text \| modify-content} | Specify the action towards hypertext markup language (HTML) tags in email messages:<br>• `convert-to-text`: Convert the HTML content to text only content.<br>• `modify-content`: Set to determine active content handling and URI processing (see `html-content-uri-selection` and `remove-active-content` respectively). | modify-content |
| html-content-uri-action {click-protection \| click-protection-isolator \| isolator \| keep \| remove} | Specify HTML content URI tag handling in email messages:<br>• `click-protection`: Rewrite the URIs and in case the user clicks on the URIs, scan the URIs and then take the configured actions.<br>• `click-protection-isolator`: Redirect to Click Protection and FortiIsolator. If the rewritten URL matched FortiIsolator URL category and passed Click Protection handling category, it is opened in FortiIsolator.<br>• `isolator`: Redirect to FortiIsolator.<br>• `keep`: Keep URI tags.<br>• `remove`: Remove URI tags. | click-protection |

| Variable | Description | Default |
|---|---|---|
| html-content-uri-selection {tag-attribute \| tag-content} | Select URIs to process from specified parts of HTML.<br>This field applies only if `html-content-action` is `modify-content`. | tag-attribute |
| image-analysis-scan {enable \| disable} | If you have purchase the adult image scan license, you can enable it to scan for adult images.<br>You can also configure the scan sensitivity and image sizes under Security > Other > Adult Image Analysis. | disable |
| max-num-of-attachment <number> | Specify how many attachments are allowed in one email message. The valid range is between 1 and 100. The default value is 10. | 10 |
| max-size <size-in-kb> | Enter the size threshold in kilobytes. Delivery of email messages greater than this size will be deferred until the period configured for oversize email.<br>To disable deferred delivery, enter `0`. | 10240 |
| max-size-option {message \| attachment} | Specify either the message or attachment for the size limit. | message |
| max-size-status {enable \| disable} | Enable to apply the maximum size limits. | disable |
| remove-active-content {enable \| disable} | Enable to remove active content.<br>This field applies only if `html-content-action` is `modify-content`. | enable |
| block-fragmented-email | Enable to detect and block fragmented email.<br>Some mail user agents, such as Outlook, are able to fragment big emails into multiple sub-messages. This is used to bypass oversize limits/scanning. | disable |
| block-password-protected-office | Enable to apply the block action configured in the content action profile if an attached MS Office document is password-protected, and therefore cannot be decompressed in order to scan its contents. | disable |
| check-archive-content | Enable to check for archived attachments. | |
| check-embedded-content | Enable to check for embedded contents.<br>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. | |
| bypass-on-smtp-auth | Enable to omit antispam scans when an SMTP sender is authenticated. | disable |
| check-html-content | Enable to detect hypertext markup language (HTML) tags and, if found:<br>apply the action profile | |

| Variable | Description | Default |
|---|---|---|
| | add `X-FEAS-ATTACHMENT-FILTER: Contains HTML tags.` to the message headers<br>This option can be used to mitigate potentially harmful HTML content such as corrupted images or files, or phishing URLs that have been specially crafted for a targeted attack, and therefore not yet identified by the FortiGuard Antispam service.<br>Depending on the action profile, for example, you could warn email users by tagging email that contains potentially dangerous HTML content, or, if you have removed the HTML tags, allow users to safely read the email to decide whether or not it is legitimate first, **without** automatically displaying and executing potentially dangerous scripts, images, or other files (automatic display of HTML content is a risk on some email clients).<br>**Caution**: **Unless** you also select `replace` for the action in the content action profile, HTML will **not** be removed, and the email will **not** be converted to plain text. Instead, the FortiMail unit will only apply whichever other action profile "block" action you have selected.<br>***To actually remove HTML tags, you must also select replace.***<br>If you select ***Replace***, all HTML tags will be removed, except for the minimum required by the HTML document type definition (DTD):<br>`<html>`<br>`<head>`<br>`<body>`<br>Stripped body text will be surrounded by `<pre>` tags, which is typically rendered in a monospace font, causing the appearance to mimic plain text.<br>For linked files, which are hosted on an external web site for subsequent download rather than directly attached to the email, the FortiMail unit will download and attach the file to the email **before** removing the `<img>` or `<embed>` tag. In this way, while the format is converted to plain text, attachments and linked files which may be relevant to the content are still preserved.<br>For example, in an email that is a mixture of HTML and plain text (`Content-Type: multipart/alternative`), and if the action profile's "block" action is `replace`, the FortiMail unit would remove hyperlink, font, and other HTML tags in the sections labeled with `Content-Type: text/html`. Linked images would be converted to attachments (The MIME `Content-Type: text/html` label itself, however, would **not** be modified). | |
| check-max-num-of-attachment | Enable to specify how many attachments are allowed in one email message. The valid range is between 1 and 100. The default value is 10. | |
| check-text-content | Enable to check the URI in the text part of the messages. | |
| defer-message-delivery | Enable to defer mail delivery from specific senders configured in policy to conserve peak time bandwidth at the expense of sending low priority, bandwidth consuming traffic at scheduled times. For example, you can apply this function to senders of marketing campaign emails or mass mailing. | |
| text-content-action {remove-uri \| click-protection} | Remove URIs: Removes URIs in the text parts of email messages.<br>Click Protection: Rewrite the URIs and in case the user clicks on the URIs, scan the URIs and then take the configured action. | remove-uri |

## Related topics

profile content-action on page 203

# 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> on page 204
      config header-insertion-list
         edit <header-insertion-name>
            set header-insertion-value <value_str>
      end
      config header-removal-list
         edit <header-removal-name>
         next
      end
      set action {discard | domain-quarantine | encryption | none | personal-
          quarantine | reject | rewrite-rcpt | system-quarantine | treat-as-spam}
          on page 204
      set alternate-host {<relay_fqdn> | <relay_ipv4>} on page 204
      set alternate-host-status {enable | disable} on page 205
      set archive-account <account_name> on page 204
      set archive-status {enable | disable} on page 204
      set bcc-addr <recipient_email>
      set bcc-env-from-addr <message_str>
      set bcc-env-from-status {enable | disable}
      set bcc-status {enable | disable} on page 205
      set deliver-to-original-host {enable | disable} on page 205
      set disclaimer-insertion {enable | disable} on page 205
      set disclaimer-insertion-content <message_name> on page 205
      set disclaimer-insertion-location {beginning | end} on page 205
      set notification-profile <profile_name> on page 206
      set notification-status {enable | disable} on page 206
      set remove-header {enable | disable}
      set replace-content {enable | disable} on page 206
```

```
        set replace-content-message on page 206
        set rewrite-rcpt-domain-type {none | prefix | replace | suffix} on page 206
        set rewrite-rcpt-domain-value <case_str> on page 206
        set rewrite-rcpt-local-type {none | prefix | replace | suffix} on page 206
        set rewrite-rcpt-local-value <value_str> on page 206
        set subject-tagging-text <text_str> on page 206
        set tagging type {insert-header | tag-subject} on page 207
end
```

| Variable | Description | Default |
|---|---|---|
| <profile_name> | Enter the name of the profile.<br>To view a list of existing entries, enter a question mark ( ? ). | |
| 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.<br>• `discard`: Accept the email, but then delete it instead of delivering the email, without notifying the SMTP client.<br>• `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.<br>• `encryption`: Apply an encryption profile.<br>• `none`: Apply any configured header or subject line tags, if any.<br>• `personal-quarantine`: Divert the email to the per-recipient quarantine.<br>• `reject`: Reject the email, replying with an SMTP error code to the SMTP client.<br>• `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} on page 206, rewrite-rcpt-domain-value <case_str> on page 206, rewrite-rcpt-local-type {none \| prefix \| replace \| suffix} on page 206, and rewrite-rcpt-local-value <value_str> on page 206.<br>• `system-quarantine`: Divert the email to the system quarantine.<br>• `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.<br>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.<br>Enable archive-status {enable \| disable} on page 204 to make this function work.<br>For more information about archive accounts, see antispam url-fgas-exempt-list on page 56. | |
| archive-status {enable \| disable} | Enable to allow the archive-account <account_name> on page 204 function to work. | disable |

| Variable | Description | Default |
|---|---|---|
| alternate-host-status {enable \| disable} | Enable to route the email to a specific SMTP server or relay. Also configure alternate-host {<relay_fqdn> \| <relay_ipv4>} on page 204.<br>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 on page 137 and the protected domain's tp-use-domain-mta {yes \| no} on page 114. | disable |
| bcc-addr <recipient_email> | Type the blind carbon copy (BCC) recipient email address.<br>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.<br>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} on page 180. | 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 |
| header-insertion-name | 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.<br>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.<br>Message header lines are composed of two parts: a key and a value, which are separated by a colon. For example, you might enter:<br>`X-Content-Filter: Contains banned word.`<br>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.<br>**Note**: Do not enter spaces in the key portion of the header line, as these are forbidden by RFC 2822.<br>Also configure tagging type {insert-header \| tag-subject} on page 207. | |
| header-removal-name | Enter the message header name to be removed. | |

| Variable | Description | Default |
|---|---|---|
| header-insertion-value <value_str> | Enter the message header value. The FortiMail unit will add this value to the message header of the email before forwarding it to the recipient.<br>Also configure tagging type {insert-header \| tag-subject} on page 207. | |
| 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 |
| remove-header {enable \| disable} | Enable removing headers defined in the header removal list.<br>Once enabled, configure header-removal-name under `config header-removal-list`. | disable |
| replace-content {enable \| disable} | Enable or disable content replacement. | disable |
| replace-content-message | Enter the name of the custom message for content replacement. | |
| 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.<br>`none`: No change.<br>`prefix`: Enter to prepend the part with new text. Also configure rewrite-rcpt-domain-value <case_str> on page 206.<br>`suffix`: Enter to append the part with new text. Also configure rewrite-rcpt-domain-value <case_str> on page 206.<br>`replace`: Enter to substitute the part with new text. Also configure rewrite-rcpt-domain-value <case_str> on page 206. | none |
| rewrite-rcpt-domain-value <case_str> | Enter the text for the option (except `none`) you choose in rewrite-rcpt-domain-type {none \| prefix \| replace \| suffix} on page 206. | |
| 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.<br>`none`: No change.<br>`prefix`: Enter to prepend the part with new text. Also configure rewrite-rcpt-local-value <value_str> on page 206.<br>`suffix`: Enter to append the part with new text. Also configure rewrite-rcpt-local-value <value_str> on page 206.<br>`replace`: Enter to substitute the part with new text. Also configure rewrite-rcpt-local-value <value_str> on page 206. | 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} on page 206. | |
| 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. | |

| 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 subject line. For details, see the documentation for your email client.<br>Also configure tagging type {insert-header \| tag-subject} on page 207. | |
| tagging type {insert-header \| tag-subject} | Enter the type of tagging for this profile. | |

## Related topics

profile encryption on page 212 on page 197

# 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 set cousin-domain-scan-option {auto-detection body-detection header-detection} for more information.

## 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. | |

| Variable | Description | Default |
|---|---|---|
| <entry_int> | Enter the entry number of the cousin domain profile.<br>If the entry profile does not currently exist, it will be created. | |
| <exempt_int> | Enter the entry number of the cousin domain profile.<br>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> on page 208
      config item
         edit <item_int> on page 208
            set pattern <pattern_str> on page 208
            set pattern-comments <comment_str> on page 209
            set pattern-type {ABAROUTING | CANSIN | CUSIP | CreditCard | ISIN |
                 USSSN | regex | wildcard} on page 209
            set pattern-weight <weight_int> on page 209
            set pattern-scan-area {header | body} on page 209
            set pattern-status {enable | disable} on page 210
            set pattern-max-weight <weight_int> on page 210
            set pattern-max-limit {enable | disable} on page 210
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.<br>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.<br>Regular expressions do not require slash (/) boundaries. For example, enter: | |

| Variable | Description | Default |
|---|---|---|
| | `v[i1]agr?a`<br>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).<br>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:<br>`=?iso-8859-1?B?U2UgdHJhdGEgZGVsIHNwYW0uCg==?=`<br>the pattern must match:<br>`Se trata del spam.`<br>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.<br>`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.<br>`CANSIN`: Canadian Social Insurance Number. The format is three groups of three digits, such as 649 242 666.<br>`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.<br>`CreditCard`: Major credit card number formats.<br>`ISIN`: An International Securities Identification Number (ISIN) uniquely identifies a security. Securities for which ISINs are issued include bonds, commercial paper, equities and warrants. The ISIN code is a 12-character alpha-numerical code that does not contain information characterizing financial instruments but serves for uniform identification of a security at trading and settlement.<br>`USSSN`: United States Social Security number. The format is a nine digit number, such as 078051111.<br>For user-defined patterns, enter either:<br>`wildcard`: Pattern is verbatim or uses only simple wild cards (`?` or `*`).<br>`regex`: Pattern is a Perl-style regular expression. | regex |
| pattern-weight <weight_int> | Enter a number by which an email's dictionary match score will be incremented for each word or phrase it contains that matches this pattern.<br>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. | |

| Variable | Description | Default |
|---|---|---|
| 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> on page 210. | disable |

## Related topics

profile dictionary-group on page 210

# 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 208.

## Syntax

```
config profile dictionary-group
   edit <group_name> on page 210
      config dictionaries
         edit <dictionary_name> on page 210
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 on page 208

# 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. | |
| 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 ms365 profile antivirus on page 151.

## Syntax

```
config profile email-address-group
   edit <group_name> on page 212
      config member
         edit <email_address> on page 212
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

ms365 profile antivirus on page 151

# 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 password <password_str> on page 145
      set encryption-algorithm {aes128 | aes192 | aes256 | cast5 | tripledes} on
          page 212
      set action-on-failure {drop | send | tls} on page 212
      set max-push-size <size_int> on page 212
      set protocol {smime | ibe} on page 212
      set retrieve-action {push | pull} on page 212
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:<br>`drop`: Send a delivery status notification (DSN) email to the sender's email address, indicating that the email is permanently undeliverable.<br>`send`: Deliver the email without encryption. | drop |
| max-push-size <size_int> | The maximum message size (in KB) of the secure mail delivered (or pushed) to the recipient. Messages that exceed this size are delivered via pull. The size cannot exceed 10240KB.<br>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 |

| Variable | Description | Default |
|---|---|---|
| | `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.<br>`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.<br>This option applies to the IBE protocol only. | |

## Related topics

profile authentication on page 191

# profile geoip-group

Use this command to create groups of GeoIP addresses.

FortiMail utilizes the GeoIP database to map the geolocations of client IP addresses. You can use GeoIP groups in access control rules and IP-based policies to geo-targeting spam and virus devices.

## Syntax

```
config profile geoip-group
   edit profile geoip-group on page 213
      set description <string>
      set country {ZZ | O1 | AD | ...}
end
```

| Variable | Description | Default |
|---|---|---|
| description <string> | Enter a description. | |
| country {ZZ \| O1 \| AD \| ...} | Assign countries to the GeoIP address group.<br>Enter `set country ?` to display all available countries. For multiple countries, separate each entry with a space. | |

# 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> on page 214
      config entry
         edit <entry> on page 214
            set display-name on page 214
            set display-name-type on page 214
            set email-address on page 214
      config exempt
         edit <entry>
            set display-name on page 214
            set display-name-type on page 214
            set email-address on page 214
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 ms365 profile antivirus on page 151.

## Syntax

```
config profile ip-address-group
   edit <name> on page 215
      config member
         edit <ip/mask> on page 215
      set comment <string>
end
```

| Variable | Description | Default |
|---|---|---|
| <name> | Enter the name of the IP address group. | |
| <ip/mask> | Enter the Enter the IP address and netmask that you want to include in the email group. Use the netmask, the portion after the slash (/), to specify the matching subnet.<br>For example, enter 10.10.10.10/24 to match a 24-bit subnet, or all addresses starting with 10.10.10. This will appear as 10.10.10.0/24 in the access control rule table, with the 0 indicating that any value is matched in that position of the address.<br>Similarly, 10.10.10.10/32 will appear as 10.10.10.10/32 and match only the 10.10.10.10 address.<br>To match any address, enter 0.0.0.0/0. | |

## Related topics

ms365 profile antivirus on page 151

# 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> on page 216
      set iprange {enable | disable} on page 216
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 preparing an LDAP directory for use with FortiMail LDAP profiles, see the FortiMail Administration Guide.

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

## Syntax

```
config profile ldap
   edit <profile_name> on page 217
      set access-override {enable | disable} on page 218
      set access-override-attribute <attribute_str> on page 218
      set address-map-state {enable | disable} on page 218
      set alias-base-dn <dn_str> on page 218
      set alias-bind-dn <bind_dn_str> on page 218
      set alias-bind-password <bindpw_str> on page 219
      set alias-dereferencing {never | always | search | find} on page 219
      set alias-expansion-level <limit_int> on page 219
      set alias-group-expansion-state {enable | disable} on page 219
      set alias-group-member-attribute <attribute_str> on page 220
      set alias-group-query <query_str> on page 220
      set alias-member-mail-attribute <attribute_str> on page 220
      set alias-member-query <query_str> on page 220
      set alias-schema {activedirectory | dominoperson | inetlocalmailrcpt |
           inetorgperson | userdefined} on page 220
      set alias-scope {base one | sub} on page 220
      set alias-state {enable | disable} on page 221
      set antispam <attribute_str> on page 221
      set webmail-language <language_name> on page 115
      set asav-state {enable | disable} on page 221
      set auth-bind-dn {cnid | none | searchuser | upn} on page 221
      set authstate {enable | disable} on page 221
      set base-dn <basedn_str> on page 221
      set bind-dn <binddn_str> on page 221
      set bind-password <bindpw_str> on page 221
      set cache-state {enable | disable} on page 222
```

```
        set cache-ttl <ttl_int> on page 222
        set set chain on page 222
        set set chain-status {enable | disable} on page 222
        set cnid-name <cnid_str> on page 222
        set content <string> on page 222
        set dereferencing {never | always | search | find} on page 222
        set display-name on page 214
        set domain-antispam-attr <attribute_str> on page 222
        set domain-antivirus-attr <attribute_str> on page 223
        set domain-content-attr on page 223
        set domain-override {enable | disable} on page 223
        set domain-override-attribute on page 223
        set domain-parent-attr <attribute_str> on page 223
        set domain-query <query_str> on page 223
        set domain-routing-mail-host-attr <attribute_str> on page 224
        set domain-state {enable | disable} on page 224
        set external-address <attribute_str> on page 224
        set fallback-port <port_int> on page 224
        set fallback-server {<fqdn_str> | <server_ipv4>} on page 224
        set group-base-dn <basedn_str> on page 224
        set group-expansion-level on page 224
        set group-membership-attribute <attribute_str> on page 224
        set quarantine-report-to-ldap-groupowner {enable | disable} on page 110
        set group-owner {enable | disable} on page 225
        set group-owner-address-attribute <attribute_str> on page 225
        set group-owner-attribute <attribute_str> on page 225
        set group-relative-name {enable | disable} on page 225
        set server-name <name_str> on page 141
        set groupstate {enable | disable} on page 226
        set internal-address <attribute_str> on page 226
        set port <port_int> on page 226
        set query <query_str> on page 226
        set rcpt-vrfy-bypass {enable | disable} on page 227
        set referrals-chase {enable | disable} on page 227
        set routing-mail-host <attribute_str> on page 227
        set routing-mail-addr <attribute_str> on page 227
        set routing-state {enable | disable} on page 228
        set schema {activedirectory | dominoperson | inetlocalmailrcpt |
             inetorgperson | userdefined} on page 228
        set scope {base | one | sub} on page 228
        set secure {none | ssl} on page 228
        set server <name_str> on page 228
        set timeout <timeout_int> on page 228
        set unauth-bind {enable | disable} on page 228
        set upn-suffix <upns_str> on page 229
        set version {ver2 | ver3} on page 229
        set webmail-password-change {enable | disable} on page 229
        set webmail-password-schema {openldap | activedirectory} on page 229
end
```

| Variable | Description | Default |
|---|---|---|
| <profile_name> | Enter the name of the LDAP profile. | |

| Variable | Description | Default |
|---|---|---|
| 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.<br>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.<br>User or alias objects should be child nodes of this location.<br>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).<br>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.<br>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`. | |

| Variable | Description | Default |
|---|---|---|
| | 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} on page 228. | |
| alias-bind-password <bindpw_str> | Enter the password of `alias-bind-dn <bind_dn_str>` on page 218. | |
| alias-dereferencing {never \| always \| search \| find} | Select the method to use, if any, when dereferencing attributes whose values are references:<br>• `never`: Do not dereference.<br>• `always`: Always dereference.<br>• `search`: Dereference only when searching.<br>• `find`: Dereference only when finding the base search object. | never |
| alias-expansion-level <limit_int> | Enter the maximum number of alias nesting levels that aliases the FortiMail unit will expand. | 0 |
| alias-group-expansion-state {enable \| disable} | Enable if your LDAP schema resolves email aliases indirectly. For more information on direct vs. indirect resolution, see `alias-base-dn <dn_str>` on page 218.<br>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.<br>When this option is **enabled**, alias resolution occurs using **two** queries:<br>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.<br>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.<br>The two-query approach is appropriate if, in your schema, alias objects are structured like group objects and contain references in the form of distinguished names of member user objects, rather than directly containing email addresses to which the alias resolves. In this case, the FortiMail unit must first “expand" the alias object into its constituent user objects before it can resolve the alias email address. | disable |

| Variable | Description | Default |
|---|---|---|
| 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.<br>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> on page 220. | |
| 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.<br>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.<br>For example, if alias objects in your directory have two distinguishing characteristics, their `objectClass` and `proxyAddresses` attributes, the query filter might be:<br>`(&(objectClass=group) (proxyAddresses=smtp:$m))`<br>where `$m` is the FortiMail variable for an email address. | |
| 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`.<br>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> on page 220, from the LDAP directory.<br>The query filter string filters the result set, and should be based upon any attributes that are common to all user/alias objects but also exclude non-user/alias objects.<br>For example, if user objects in your directory have two distinguishing characteristics, their `objectClass` and `mail` attributes, the query filter might be:<br>`(& (objectClass=alias) (mail=$m))`<br>where `$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:<br>• `base`: Query the `basedn` level.<br>• `one`: Query only the one level directly below the `basedn` in | sub |

| Variable | Description | Default |
|---|---|---|
| | the LDAP directory tree.<br>• `sub`: Query recursively all levels below the `basedn` in the LDAP directory tree. | |
| 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. | |
| 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:<br>`cnid`: Enter the name of the user objects' common name attribute, such as `cn` or `uid`.<br>`searchuser`: Enter to form the user's bind DN by using the DN retrieved for that user<br>This command applies only if `schema` is `userdefined` in "set ldap_profile profile user" on page 2407..<br>`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`).<br>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> on page 229`. | searchuser |
| authstate {enable \| disable} | Enable to perform user authentication queries. | disable |
| base-dn <basedn_str> | Enter the distinguished name (DN) of the part of the LDAP directory tree within which the FortiMail unit will search for user objects, such as `ou=People,dc=example,dc=com`.<br>User objects should be child nodes of this location. | |
| bind-dn <binddn_str> | Enter the bind DN, such as `cn=FortiMailA,dc=example,dc=com`, of an LDAP user account with permissions to query the `basedn`.<br>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} on page 228. | |
| bind-password <bindpw_str> | Enter the password of `bind-dn <binddn_str> on page 221`. | |

| Variable | Description | Default |
|---|---|---|
| cache-state {enable \| disable} | Enable to cache LDAP query results.<br>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.<br>If this option is enabled but queries are not being cached, inspect the value of TTL. Entering a TTL value of `0` effectively disables caching. | disable |
| cache-ttl <ttl_int> | Enter the amount of time, in minutes, that the FortiMail unit will cache query results. After the TTL has elapsed, cached results expire, and any subsequent request for that information causes the FortiMail unit to query the LDAP server, refreshing the cache.<br>The default TTL value is 1,440 minutes (one day). The maximum value is 10,080 minutes (one week). Entering a value of `0` effectively disables caching. | 1440 |
| set chain | Enter the LDAP profile you wish to add the group of other LDAP profiles to create a chain query. | |
| set chain-status {enable \| disable} | Enable the chain query. | disable |
| cnid-name <cnid_str> | Enter the name of the user objects' common name attribute, such as `cn` or `uid`. | |
| content <string> | Enter the name of the attribute, such as `genericContent`, whose value is the name of the content profile assigned to the domain.<br>The name of this attribute may vary by the schema of your LDAP directory.<br>If you do not specify this attribute at all (that is, leave this field blank), the content profile in the matched recipient-based policy will be used. | |
| dereferencing {never \| always \| search \| find} | Select the method to use, if any, when dereferencing attributes whose values are references.<br>• `never`: Do not dereference.<br>• `always`: Always dereference.<br>• `search`: Dereference only when searching.<br>• `find`: Dereference only when finding the base search object. | never |
| display-name | 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. | |

| Variable | Description | Default |
|---|---|---|
| | 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.<br>The name of this attribute may vary by the schema of your LDAP directory. | |
| domain-content-attr | Enter the content attribute name. | |
| domain-override {enable \| disable} | Enable or disable system admin domain override. | |
| domain-override-attribute | Enter the system admin domain ovveride attribute. | |
| domain-parent-attr <attribute_str> | Enter the name of the parent domain attribute, such as `description`, whose value is the name of the parent domain from which a domain inheritate the specific RCPT check settings and quarantine report settings.<br>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.<br>For details on query syntax, refer to any standard LDAP query filter reference manual.<br>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.<br>The user entry should be configured with attributes to represent the following:<br>• parent domain from which a domain inherits the specific RCPT check settings and quarantine report settings. For example, `description=parent.com`<br>• IP address of the backend mail server hosting the mailboxes of the domain. For example, `mailHost=192.168.1.105`<br>• antispam profile assigned to the domain. For example, `businessCategory=parentAntispam`<br>• antivirus profile assigned to the domain. For example, `preferredLanguage=parentAntivirus` | |

| Variable | Description | Default |
|---|---|---|
| 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.<br>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.<br>For more information about domain lookup, see domain-query <query_str> on page 223. | disable |
| external-address <attribute_str> | Enter the name of the attribute, such as `externalAddress`, whose value is an email address in the same or another protected domain.<br>This email address will be rewritten into the value of `internal-address <attribute_str> on page 226` according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings: on page 230.<br>The name of this attribute may vary by the schema of your LDAP directory. | extAddress |
| fallback-port <port_int> | If you have configured a backup LDAP server that listens on a nonstandard port number, enter the TCP port number.<br>The standard port number for LDAP is 389. The standard port number for SSL-secured LDAP is 636.<br>The FortiMail unit will use SSL-secured LDAP to connect to the server if `secure` is `ssl`. | 389 |
| fallback-server {<fqdn_str> \| <server_ipv4>} | Enter either the fully qualified domain name (FQDN) or IP address of the backup LDAP server.<br>If there is no fallback server, enter an empty string ( " ). | |
| group-base-dn <basedn_str> | Enter the base DN portion of the group's full DN, such as `ou=Groups,dc=example,dc=com`.<br>This command applies only if `group-relative-name` is `enable`. | |
| group-expansion-level | 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.<br>This attribute must be present in user objects. | |

| Variable | Description | Default |
|---|---|---|
| | 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.<br>This command applies only if `group-relative-name` is `enable`. | |
| group-owner {enable \| disable} | Enable to query the group object by its distinguished name (DN) to retrieve the DN of the group owner, which is a user that will receive that group's spam reports. Using that user's DN, the FortiMail unit will then perform a second query to retrieve that user's email address, where the spam report will be sent.For more information on sending spam reports to the group owner, see config domain-setting on page 105. | 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.<br>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.<br>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.<br>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. | disable |

| Variable | Description | Default |
|---|---|---|
| | 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.<br>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 <basedn_str> on page 221 as if they were members of a user group object.<br>For example, your LDAP directory might not contain user group objects. In that sense, groups do not really exist in the LDAP directory. However, you could mimic a group's presence by enabling this option to treat all users that are child objects of the base DN in the user object query as if they were members of such a group. | disable |
| groupstate {enable \| disable} | Enable to perform LDAP group queries. | disable |
| internal-address <attribute_str> | Enter the name of the LDAP attribute, such as `internalAddress`, whose value is an email address in the same or another protected domain.<br>This email address will be rewritten into the value of `external-address <attribute_str> on page 224` according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings: on page 230.<br>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.<br>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.<br>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.<br>For example, if user objects in your directory have two distinguishing characteristics, their `objectClass` and `mail` attributes, the query filter might be:<br>`(& (objectClass=inetOrgPerson) (mail=$m))`<br>where `$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:<br>`(& (objectClass=inetOrgPerson) (mail=$m${-spam}))`<br>where `${-spam}` is the FortiMail variable for the tag to remove before performing the query. Similarly, to subtract "spam-" from the **beginning** of the user name portion of the recipient email address, you could use the query filter:<br>`(& (objectClass=inetOrgPerson) (mail=$m${^spam-}))`<br>where `${^spam-}` is the FortiMail variable for the tag to remove before performing the query.<br>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.<br>For details on query syntax, refer to any standard LDAP query filter reference manual.<br>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. | disable |
| referrals-chase {enable \| disable} | Enable chase 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, such as `mailRoutingAddress`, 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.<br>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.<br>If you enter `userdefined`, you must configure `query`. | inetorgperson |
| scope {base \| one \| sub} | Enter which level of depth to query:<br>`base`: Query the `basedn` level.<br>`one`: Query only the one level directly below the `basedn` in the LDAP directory tree.<br>`sub`: Query recursively all levels below the `basedn` in the LDAP directory tree. | sub |
| secure {none \| ssl} | Enter a value to indicate whether or not to connect to the LDAP server(s) using an encrypted connection.<br>none: Use a non-secure connection.<br>SSL: Use an SSL-secured (LDAPS) connection.<br>Note: If your FortiMail unit is deployed in server mode, and you want to enable webmail-password-change {enable \| disable} on page 229 using an LDAP server that uses a Microsoft ActiveDirectory-style schema, you must select ***SSL***. ActiveDirectory servers require a secure connection for queries that change user passwords. | none |
| server <name_str> | Enter the fully qualified domain name (FQDN) or IP address of the LDAP server. | |
| timeout <timeout_int> | Enter the maximum amount of time in seconds that the FortiMail unit will wait for query responses from the LDAP server. | 10 |
| unauth-bind {enable \| disable} | 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. | disable |

| Variable | Description | Default |
|---|---|---|
| | 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 backend 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.<br>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.<br>***Note***: This option is available in CLI only. And it only takes effect for webmail access in gateway and transparent mode. | |
| upn-suffix <upns_str> | If you want to use a UPN other than the mail domain, enter that UPN. This can be useful if users authenticate with a domain other than the mail server's principal domain name. | |
| version {ver2 \| ver3} | Enter the version of the protocol used to communicate with the LDAP server. | ver3 |
| webmail-password-change {enable \| disable} | Enable to perform password change queries for FortiMail webmail users. | disable |
| webmail-password-schema {openldap \| activedirectory} | Enter one of the following to indicate the schema of your LDAP directory:<br>`openldap`: The LDAP directory uses an OpenLDAP-style schema.<br>`activedirectory`: The LDAP directory uses a Microsoft Active Directory-style schema.<br>Note: Microsoft Active Directory requires that password changes occur over an SSL-secured connection. | openldap |

## Email address mapping

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

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

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

- Mappings cannot translate one email address into many.
- Mappings cannot translate an email address into one that belongs to an unprotected domain (this restriction applies to locally defined address mappings only; 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:<br>`MAIL FROM:`<br>`RCPT TO:`<br>`From:`<br>`To:`<br>`Return-Path:`<br>`Cc:`<br>`Reply-To:`<br>`Return-Receipt-To:`<br>`Resent-From:`<br>`Resent-Sender:`<br>`Delivery-Receipt-To:`<br>`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.

## Related topics

profile authentication on page 191

# 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:<br>• `host`: Relay matched session to specified SMTP server.<br>• `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.<br>If there are multiple MX records, FortiMail will load balance between them.<br>• `mx-lookup-match-domain`: Relay through the MX record lookup of the matched recipient domain.<br>• `relay-host`: Relay to a pre-defined relay host. | 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> on page 232
      set attach-original-message {enable | disable} on page 232
      set email-template <template_name> on page 232
      set other <recipient_address> on page 232
      set recipient {none | other | recipient | sender} on page 232
      set type {generic | sender_addr_rate_ctrl} on page 232
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:<br>• content-subject<br>• content-body<br>• content-attachment-blocked<br>• content-attachment-number-limit-exceeded<br>• content-attachment-size-limit-exceeded<br>• content-size-limit-exceeded<br>• dlp-subject<br>• dlp-body<br>• dlp-attachment<br>• virus-body<br>• virus-attachment-infected<br>• virus-attachment-suspicious | |
| content <string> | Enter the content of the specific replacement message.<br>Note there is a 8191 character limit for each replacement 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> on page 234
    set auto-check-message on page 234
    set auto-delete-old-mail <days> on page 234
    set auto-delete-sent-folder <days>
    set auto-delete-trash-folder <days> on page 234
    set auto-forward {enable | disable} on page 234
    set auto-reply {enable | disable} on page 234
    set email-continuity-status {enable | disable}
    set idle-timeout {enable | disable}
    set message-filter {enable | disable} on page 234
    set mobile-access {enable | disable} on page 234
```

```
        set outbound-safelist on page 234
        set quarantine-bcc-addr on page 234
        set quarantine-bcc-status on page 234
        set quarantine-days on page 235
        set quarantine-report {enable | disable} on page 235
        set quota <number_mb> on page 235
        set release-auto-safelist on page 235
        set release-through-email on page 235
        set release-through-web on page 235
        set status {enable | disable} on page 235
        set webmail-access {enable | disable} on page 235
        set webmail-addressbook-access {domain | none | system} on page 235
        set profile resource on page 233
end
```

| Variable | Description | Default |
|---|---|---|
| auto-check-message | Enable or disable auto checking new messages in 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 |
| 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 (license based).<br>When the SMTP server is detected as inaccessible, recipient verification is skipped and emails are put into the email continuity queue. When the SMTP server is accessible again, the email is delivered. Note there is no DSN if the email is from an unknown user. | enable |
| idle-timeout {enable \| disable} | Enable to enforce an idle timeout in webmail | enable |
| message-filter {enable \| disable} | Enable to allow message filtering in webmail. | enable |
| mobile-access {enable \| disable} | Enble 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 |

| Variable | Description | Default |
|---|---|---|
| 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 <number_mb> | Enter the user's disk space quota in Megabytes. | 1000 |
| release-auto-safelist | Automatically add sender of a released message to personal safelist. | enable |
| release-through-email | Enable or disable auto release quarantined emails through email | disable |
| release-through-web | Enable or disable auto release quarantined emails through the web. | enable |
| 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} | Use this command to turn on/off the user preference option on the 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> on page 237
    set access-control <profile_name>
    set block_encrypted {enable | disable} on page 237
    set bypass-bounce-verification {enable | disable} on page 237
    set check-client-ip-quick {enable | disable} on page 238
    set conn-blocklisted {enable | disable} on page 238
    set conn-concurrent <connections_int> on page 238
    set conn-hiden {enable | disable} on page 238
    set conn-idle-timeout <timeout_int> on page 238
```

```
set conn-total <connections_int> on page 239
set dkim-signing {enable | disable} on page 239
set dkim-signing-authenticated-only {enable | disable} on page 239
set dkim-validation {enable | disable} on page 239
set domain-key-validation {enable | disable} on page 239
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} on page 239
set endpoint-reputation {enable | disable} on page 239
set endpoint-reputation-action {reject | monitor} on page 240
set endpoint-reputation-blocklist-duration <duration_int> on page 240
set endpoint-reputation-blocklist-trigger <trigger_int> on page 240
set eom-ack {enable | disable} on page 240
set error-drop-after <errors_int> on page 240
set error-penalty-increment <penalty-increment_int> on page 240
set error-penalty-initial <penalty-initial_int> on page 240
set error-penalty-threshold <threshold_int> on page 240
set fortiguard-ip-check-mode {as-profile | as-profile-no-auth | client-
    connect | disable}
set limit-NOOPs <limit_int> on page 241
set limit-RSETs <limit_int> on page 241
set limit-email <limit_int> on page 241
set limit-helo <limit_int> on page 241
set limit-max-header-size <limit_int> on page 241
set limit-max-message-size <limit_int>
set limit-recipient <limit_int> on page 241
set mail-route <profile_name> on page 241
set number-of-messages <limit_int> on page 241
set number-of-recipients <limit_int> on page 242
set recipient-blocklist-status {enable | disable} on page 242
set recipient-rewrite-map <profile_name> on page 242
set recipient-safelist-status {enable | disable} on page 242
set remote-log <profile_name> on page 242
set remove-current-headers {enable | disable}
set remove-headers {enable | disable} on page 242
set remove-received-headers {enable | disable} on page 242
set sender-blocklist-status {enable | disable} on page 242
set sender-reputation-reject-score <threshold_int> on page 242
set sender-reputation-status {enable | disable} on page 242
set sender-reputation-tempfail-score <threshold_int> on page 242
set sender-reputation-throttle-number <rate_int> on page 243
set sender-reputation-throttle-percentage <percentage_int> on page 243
set sender-reputation-throttle-score <threshold_int> on page 243
set sender-rewrite-map <profile_name>
set sender-safelist-status {enable | disable} on page 243
set sender-verification {enable | disable}
set sender-verification-profile <profile_name>
set session-3way-check {enable | disable} on page 243
set session-action <content-action_profile>
set session-action-msg-type {accepted | all}
set session-allow-pipelining {yes | no} on page 243
set session-command-checking {enable | disable} on page 244
set session-disallow-encrypted {enable | disable} on page 244
set session-helo-char-validation {enable | disable} on page 244
set session-helo-domain-check {enable | disable} on page 244
set session-helo-rewrite-clientip {enable | disable} on page 245
set session-helo-rewrite-custom {enable | disable} on page 245
```

```
      set session-helo-rewrite-custom-string <helo_str> on page 245
      set session-prevent-open-relay {enable | disable} on page 245
      set session-recipient-domain-check {enable | disable} on page 245
      set session-reject-empty-domain {enable | disable} on page 246
      set session-sender-domain-check {enable | disable} on page 246
      set spf-validation {enable | disable} on page 246
      set splice-status {enable | disable} on page 246
      set splice-threshold on page 246
      set splice-unit {seconds | kilobytes} on page 247
      config header-removal-list
        edit <key_str> on page 237
      config recipient-blocklist
        edit <recipient_address_str> on page 237
      config recipient-safelist
        edit <recipient_address_str> on page 237
      config sender-blocklist
        edit <sender_address_str> on page 237
      config sender-safelist
        edit <sender_address_str> on page 237
    next
  end
```

| Variable | Description | Default |
|---|---|---|
| <profile_name> | Enter the name of the session profile. | |
| <key_str> | Enter a header key to remove it from email messages. | |
| <recipient_address_str> | Enter a blocklisted recipient email address to which this profile is applied. | |
| <recipient_address_str> | Enter a safelisted recipient email address to which this profile is applied. | |
| <sender_address_str> | Enter a blocklisted sender email address to which this profile is applied. | |
| <sender_address_str> | Enter a safelisted sender email address to which this profile is applied. | |
| access-control <profile_name> | **Note:** This feature is only available as part of the MTA advanced control feature. See `mta-adv-ctrl-status` under system global on page 287<br>Enter an access control profile to be used in a session profile. | |
| block_encrypted {enable \| disable} | Enable to block TLS/MD5 commands so that email must pass unencrypted, enabling the FortiMail unit to scan the email for viruses and spam.<br>Disable to pass TLS/MD5 commands, allowing encrypted email to pass. The FortiMail unit cannot scan encrypted email for viruses and spam.<br>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.<br>This bypass does not omit bounce address tagging of outgoing email.<br>Alternatively, you can omit bounce verification according to the protected domain. For details, see config domain-setting on page 105. | disable |

| Variable | Description | Default |
|---|---|---|
| | For information on enabling bounce address tagging and verification (BATV), see antispam bounce-verification on page 42. | |
| 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.<br>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.<br>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.<br>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.<br>To disable the limit, enter `0`. | 0 |
| conn-hiden {enable \| disable} | Enter either of the following transparency behaviors:<br>`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.<br>`disable`: Do not be transparent. Replace the SMTP client's IP addresses or domain names with that of the FortiMail unit.<br>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.<br>**Note:** Unless you have enabled `exclusive {enable \| disable} on page 161` in config policy delivery-control on page 159, the hide (`tp-hidden {no \| yes} on page 113`) option in config domain-setting on page 105 has precedence over this option, and may prevent it from applying to incoming email messages.<br>**Note:** For full transparency, also set the hide (`tp-hidden {no \| yes} on page 113`) option in config domain-setting on page 105 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.<br>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).<br>You set the time interval using the command:<br>`config antispam settings`<br>`  set session-profile-rate-control-interval <minutes>`<br>`end`<br>To disable the limit, enter `0`. | 0 |

| Variable | Description | Default |
|---|---|---|
| conn-total <connections_int> | Enter a limit to the total number of concurrent connections from all sources.<br>To disable the limit, enter `0`. | 0 |
| dkim-signing {enable \| disable} | Enable to sign outgoing email with a DKIM signature.<br>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.<br>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.<br>An invalid signature increases the client sender reputation score and affect the deep header scan. A valid signature decreases the client sender reputation score.<br>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.<br>An unauthorized client IP address increases the client sender reputation score. An authorized client IP address decreases the client sender reputation score.<br>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. | |
| email-queue {default \| incoming \| no-preference \| outgoing} | **Note:** This feature is only available as part of the MTA advanced control feature. See `mta-adv-ctrl-status` under system global on page 287<br>Enter the email queue to use for the matching sessions. | no-preference |
| endpoint-reputation {enable \| disable} | Enable to accept, monitor, or reject email based upon endpoint reputation scores.<br>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 242. | disable |

| Variable | Description | Default |
|---|---|---|
| endpoint-reputation-action {reject \| monitor} | Enter either:<br>`reject`: Reject email and MMS messages from MSISDNs/subscriber IDs whose MSISDN reputation scores exceed ***Auto blocklist score trigger value***.<br>`monitor`: Log, but do not reject, email and MMS messages from MSISDNs/subscriber IDs whose MSISDN reputation scores exceed `endpoint-reputation-blocklist-trigger` value. 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.<br>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.<br>If the FortiMail unit has not yet completed antispam scanning by the time that four (4) minutes has elapsed, it will return SMTP reply code 451(`Try again later`), resulting in no permanent problems, as according to RFC 2281, the minimum timeout value should be 10 minutes. However, in rare cases where the server or client's timeout is shorter than 4 minutes, the sending client or server could time-out while waiting for the FortiMail unit to acknowledge the EOM command. Enabling this option prevents those rare cases. | disable |
| error-drop-after <errors_int> | Enter the total number of errors the FortiMail unit will accept before dropping the connection. | 5 |
| error-penalty-increment <penalty-increment_int> | Enter the number of seconds by which to increase the delay for each error after the first delay is imposed. | 1 |
| 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:<br>• `as-profile`: Uses the settings of the FortiGuard IP reputation in the antispam profile.<br>• `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. | as-profile |

| Variable | Description | Default |
|---|---|---|
| | • `client-connect`: Checks FortiGuard IP reputation the moment a client connects.<br>• `disable`: Disables FortiGuard IP reputation check. | |
| limit-NOOPs <limit_int> | Enter the limit of NOOP commands that are permitted per SMTP session. Some spammers use NOOP commands to keep a long session alive. Legitimate sessions usually require few NOOPs.<br>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 RSETs.<br>To disable the limit, enter `0`. | 20 |
| limit-email <limit_int> | Enter the limit of email messages per session to prevent mass mailing.<br>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.<br>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 |
| limit-max-message-size <limit_int> | Enter the limit of the message size. If enabled, messages over the threshold size are rejected. | 10240 |
| limit-max-message-size <limit_int> | Enter the limit of message size in kilobytes (KB) . If enabled, messages over the threshold size are rejected.<br>**Note**: If both this option and `max-message-size <limit_int> on page 109` in the protected domain are enabled, email size will be limited to whichever size is smaller. | 10240KB |
| 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 (the default value is 30 minutes).<br>You set the time interval using the command:<br>`config antispam settings`<br>`  set session-profile-rate-control-interval <minutes>`<br>`end`<br>Enter 0 to disable the limit. | 0 |

| Variable | Description | Default |
|---|---|---|
| number-of-recipients <limit_int> | Enter the number jof recipients per client per time interval (the default value is 30 minutes).<br>You set the time interval using the command:<br>`config antispam settings`<br>`  set session-profile-rate-control-interval <minutes>`<br>`end`<br>Enter 0 to disable the limit. | 0 |
| 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 <recipient_address_str> on page 237. | disable |
| recipient-rewrite-map <profile_name> | **Note:** This feature is only available as part of the MTA advanced control feature. See `mta-adv-ctrl-status` under system global on page 287<br>Enter an address rewrite profile to be used in a session profile. | |
| 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 <recipient_address_str> on page 237. | disable |
| remote-log <profile_name> | **Note:** This feature is only available as part of the MTA advanced control feature. See `mta-adv-ctrl-status` under system global on page 287<br>Enter a remote logging profile. Note that the remote logging profiles used here are the same as the system-wide remote logging profiles. | |
| remove-current-headers {enable \| disable} | Enable to remove headers that are inserted by the current unit.<br>**Note**: This command is enabled by default for backwards compatibility with related subcommands `remove-headers` and `remove-received-headers`. | enable |
| remove-headers {enable \| disable} | Enable to remove other configured headers from email messages. | disable |
| remove-received-headers {enable \| disable} | Enable to remove all `Received:` message headers from email messages. | disable |
| sender-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 <sender_address_str> on page 237. | 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.<br>This option applies only if sender-reputation-status {enable \| disable} on page 242 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.<br>This option applies only if sender-reputation-status {enable \| disable} on page 242 is enabled. | 55 |

| Variable | Description | Default |
|---|---|---|
| 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.<br>The enforced rate limit is either `sender-reputation-throttle-number <rate_int>` on page 243 or `sender-reputation-throttle-percentage <percentage_int>` on page 243 whichever value is greater.<br>This option applies only if sender-reputation-status {enable \| disable} on page 242 is enabled. | 15 |
| sender-rewrite-map <profile_name> | **Note:** This feature is only available as part of the MTA advanced control feature. See `mta-adv-ctrl-status` under system global on page 287<br>Enter an address rewrite profile to be used in a session profile. | |
| 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 <sender_address_str> on page 237. | 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.<br>Mismatching domain names is sometimes used by spammers to mask the true identity of their SMTP client.<br>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 one of the following behaviors for ESMTP command pipelining, which causes some SMTP commands to be accepted and processed as a batch, increasing performance over high-latency connections. | yes |

| Variable | Description | Default |
|---|---|---|
| | When set to `no`, FortiMail unit accepts only one command at a time during an SMTP session and will not accept the next command until it completes processing of the previous command.<br>This option is available for gateway, server, and transparent mode. | |
| 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.<br>`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.<br>In the following example, the invalid commands are highlighted in bold:<br>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:41:15 GMT<br>EHLO example.com<br>250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you<br>***RCPT TO:<user1@example.com>***<br>503 5.0.0 Need MAIL before RCPT | disable |
| 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.<br>Clear to pass TLS/MD5 commands, allowing encrypted email to pass. The FortiMail unit cannot scan encrypted email for viruses and spam.<br>**Note:** 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.<br>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.<br>In the following example, the invalid command is highlighted in bold:<br>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:30:20 GMT<br>***EHLO ^^&^&^#$***<br>501 5.0.0 Invalid domain name<br>Valid characters for domain names include:<br>• alphanumerics (A to Z and 0 to 9)<br>• brackets ( `[` and `]` )<br>• periods ( `.` )<br>• dashes ( `-` )<br>• underscores ( `_` )<br>• number symbols( `#` )<br>• 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. | disable |

| Variable | Description | Default |
|---|---|---|
| | 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.<br>In the following example, the invalid command is highlighted in bold:<br>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 13:30:20 GMT<br>EHLO ^^&^&^#$<br>501 5.0.0 Invalid domain name<br>Valid domain characters include:<br>• alphanumerics (A to Z and 0 to 9)<br>• brackets ( [ and ] )<br>• periods ( . )<br>• dashes ( - )<br>• underscores ( _ )<br>• number symbols( # )<br>• 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.<br>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> on page 245.<br>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.<br>This feature:<br>• applies only if the FortiMail unit is operating in transparent mode,<br>• only affects unauthenticated sessions, and<br>• is applicable only if you allow clients to use an unprotected SMTP server for outgoing connections. For details, see mailsetting proxy-smtp on page 136. | 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.<br>In the following example, the invalid command is highlighted in bold:<br>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 14:48:32 GMT<br>EHLO example.com<br>250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you<br>MAIL FROM:<user1@fortinet.com><br>250 2.1.0 <user1@fortinet.com>... Sender ok | disable |

| Variable | Description | Default |
|---|---|---|
| | ***RCPT TO:<user2@example.com>***<br>550 5.7.1 <user2@example.com>... Relaying denied. IP name lookup failed [192.168.1.1]<br>This check only affects unauthenticated sessions. | |
| 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.<br>Because the sender address is invalid and therefore cannot receive delivery status notifications (DSN), you may want to disable this feature.<br>In the following example, the invalid command is highlighted in bold:<br>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2007 14:48:32 GMT<br>EHLO example.com<br>250-FortiMail-400.localdomain Hello [192.168.171.217], pleased to meet you<br>***MAIL FROM:<john@>***<br>553 5.1.3 <john@>... Hostname required<br>This check only affects unauthenticated sessions. | disable |
| session-sender-domain-check {enable \| disable} | Enable o return SMTP reply code 421, rejecting the SMTP command, if the domain name portion of the sender address is not a domain name that exists in either MX or A records.<br>In the following example, the invalid command is highlighted in bold:<br>220 FortiMail-400.localdomain ESMTP Smtpd; Wed, 14 Feb 2008 14:32:51 GMT<br>EHLO<br>250-FortiMail-400.localdomain Hello [192.168.1.1], pleased to meet you<br>***MAIL FROM:<user1@example.com>***<br>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.<br>An unauthorized client IP address increases the client sender reputation score. An authorized client IP address decreases the client sender reputation score.<br>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.<br>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.<br>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.<br>**Note:** This option applies only if the FortiMail unit is operating in transparent mode. | disable |
| splice-threshold <integer> | Enter a threshold value to switch to splice mode based on time (seconds) or data size (kilobytes) using splice-unit {seconds \| kilobytes} on page 247. | 0 |

| Variable | Description | Default |
|---|---|---|
| | **Note:** This option applies only if the FortiMail unit is operating in transparent mode. | |
| splice-unit {seconds \| kilobytes} | Enter the time (seconds) or data size (kilobytes) for the `splice threshold`.<br>**Note:** This option applies only if the FortiMail unit is operating in transparent mode. | seconds |

## Related topics

profile encryption on page 212 on page 197

# profile tls

Use this command to configure TLS profiles that can be used by receive rules (also called access control rules) and delivery rules. Note that many subcommands are only available when `level` is set to either `preferred` or `secure`.

## Syntax

```
config profile tls
   edit <profile_name> on page 247
      set level {none | preferred | secure} on page 247
      set action {fail | tempfail} on page 248
      set ca-name <string>
      set cert-subject <string>
      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 <integer>
      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.<br>• `none`: Disables TLS. Requests for a TLS connection will be ignored.<br>• `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.<br>• `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 | none |

| Variable | Description | Default |
|---|---|---|
| | Administration Guide. | |
| action {fail \| tempfail} | Select the action the FortiMail unit takes when a TLS connection cannot be established.<br>This option does not apply for profiles whose `level` is `preferred`. | tempfail |
| ca-name <string> | Enter the name of the CA issuer.<br>This option is only available when `level` is set to `secure`. | |
| cert-subject <string> | Enter the certification subject.<br>This option is only available when `level` is set to `secure`. | |
| check-ca-name {enable \| disable} | Enable to check the CA issuer name.<br>This option is only available when `level` is set to `secure`. | disable |
| check-ca-type {match \| substring \| wildcard} | Select a CA issuer check type.<br>This option is only available when `level` is set to `secure`. | match |
| check-cert-subject {enable \| disable} | Enable to check the certificate subject name.<br>This option is only available when `level` is set to `secure`. | disable |
| check-cert-type {match \| substring \| wildcard} | Select a certificate check type.<br>This option is only available when `level` is set to `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. | disable |
| dane-support {mandatory \| none \| opportunistic} | Assign a DNS-based Authentication of Named Entities (DANE) support level.<br>Note that `mandatory` is only applicable when `level` is set to `secure`.<br>For more information, see RFC 7929. | none |
| encryption-strength <integer> | 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.<br>This option is only available when `check-ssl-version` is set to `enable`. | tls1_1 |

| Variable | Description | Default |
|---|---|---|
| mtasts-status {enable \| monitor \| none} | **Note:** The MTA-STS status may only be set when `smtp-mtasts-status` is enabled under system mailserver.<br>Enable MTA Strict Transport Security (MTA-STS) domain checking.<br>This option is only available when `level` is set to either `preferred` or `secure`. | none |

## Related topics

ms365 profile antivirus on page 151

# profile uri-filter

Use this command to configure FortiGuard URI filter profiles.

## Syntax

```
config profile uri-filter
   edit <profile_name> on page 249
      set category <filter_category> on page 249
end
```

| Variable | Description | Default |
|---|---|---|
| <profile_name> | Enter the name of the URI profile. | |
| category <filter_category> | Specify the FortiGuard URI category to use for the filter.<br>To view all available categories, enter `set category ?`. | child-abuse drug-abuse adult-materials nudity-risque pornography spam-urls phishing malicious-web |

# 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> on page 250
```

```
        set dest-ip-mask <ip/netmask_str> on page 250
        set dest-ip-type {ip-group | ip-mask} on page 250
        set direction {both | incoming | outgoing} on page 250
        set domains {all | <protected-domain_str>} on page 250
        set file-format {html | pdf} on page 250
        set period-absolute-from <start_str> on page 250
        set period-absolute-to <end_str> on page 250
        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} on page 251
        set period-relative-value <n_int> on page 251
        set query-status <query_str> on page 251
        set recipients <recipient_str> on page 251
        set schedule {daily | dates | none | weekdays} on page 251
        set schedule-dates <dates_str> on page 251
        set schedule-hour <time_int> on page 251
        set schedule-weekdays <days_str> on page 252
        set sender-domains on page 252
end
```

| Variable | Description | Default |
|---|---|---|
| <profile_name> | Enter the name of the report 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:<br>`both`: Report on both incoming and outgoing email.<br>`incoming`: Report only on email whose recipient is a member of a protected domain.<br>`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.<br>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. | |

| Variable | Description | Default |
|---|---|---|
| | 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>` on page 251. | |
| 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`.<br>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.<br>`daily`: Generate the report every day.<br>`dates`: Generate the report on certain dates in the month. Also configure schedule-dates <dates_str> on page 251.<br>`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.<br>`weekdays`: Generate the report on certain days of the week. Also configure schedule-weekdays <days_str> on page 252. | |
| 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. | |

| Variable | Description | Default |
|---|---|---|
| | For example, to generate reports at 5 PM, you would enter `17`. | |
| schedule-weekdays <days_str> | Enter the days to generate the reports. Separate each day with a comma ( , ). For example, to generate a report on Friday and Wednesday, you would enter `wednesday,friday`. | |
| sender-domains | Enter the selected sender domain names (empty means ALL) | |

## Related topics

log alertemail setting on page 131

# 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> on page 252
      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`.<br>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`.<br>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> on page 254
        config document on page 254
           edit <document id> on page 254
              set filename on page 254
              set signature on page 254
config sensitive-data fingerprint-source
     edit <DLP server name> on page 254
        set file-path on page 254
        set file-pattern on page 254
        set keep-modified on page 254
        set password on page 254
        set period on page 254
        set remove-deleted on page 254
        set scan-subdirectories on page 254
        set server on page 254
        set server-type on page 254
        set username on page 254
     edit linux on page 254
        set file-path on page 254
        set file-pattern on page 254
        set keep-modified on page 254
        set password on page 254
        set period on page 254
        set remove-deleted on page 254
        set scan-subdirectories on page 254
```

```
        set server on page 254
        set server-type on page 254
        set username on page 254
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 to which an administrator account is assigned, govern which areas of the web-based manager and CLI that an administrator can access, and whether or not they have the permissions necessary to change the configuration or otherwise modify items in each area.

## Syntax

```
config system accprofile
   edit <profile_name> on page 255
      config menuitem
         edit <name>
            set permission {custom | none | read | read-write}
            set content-detail {enable | disable}
         next
      end
```

```
        set admin {none | read | read-write}
        set archive {none | read | read-write} on page 255
        set block-safe-list {none | read | read-write} on page 255
        set granular-group {all}
        set greylist {none | read | read-write} on page 256
        set log {none | read | read-write}
        set ms365 {none | read | read-write}
        set others {none | read | read-write} on page 256
        set personal-quarantine {none | read | read-write} on page 256
        set policy {none | read | read-write} on page 256
        set privilege-level {high | low | medium}
        set queue {none | read | read-write}
        set system {none | read | read-write} on page 256
        set system-diagnostics {enable | disable}
        set system-quarantine {none | read | read-write} on page 256
end
```

| Variable | Description | Default |
|---|---|---|
| <profile_name> | Enter the name of the access profile. | |
| <name> | Enter the name of the menu item you wish to configure administrative permissions:<br>• archive_grp<br>• cluster_grp<br>• content_grp<br>• dashboard_grp<br>• domain_grp<br>• encryption_grp<br>• fortiview_grp<br>• log_grp<br>• monitor_grp<br>• ms365_grp<br>• others_grp<br>• policy_grp<br>• profile_grp<br>• security_grp<br>• system_grp | |
| permission {custom \| none \| read \| read-write} | Apply a permission across all access control configurations. | none |
| content-detail {enable \| disable} | Note that this is only available for archive_grp. | enable |
| admin {none \| read \| read-write} | For the admin configuration, enter the permissions that will be granted to administrator accounts associated with this access profile. | none |
| archive {none \| read \| read-write} | For the archiving configuration, enter the permissions that will be granted to administrator accounts associated with this access profile. | none |
| block-safe-list {none \| read \| read-write} | For the block and safelist configuration, enter the permissions that will be granted to administrator accounts associated with this access profile. | none |

| Variable | Description | Default |
|---|---|---|
| granular-group {all} | Access permission for granular control. | all |
| greylist {none \| read \| read-write} | For the greylist configuration, enter the permissions that will be granted to administrator accounts associated with this access profile. | none |
| log {none \| read \| read-write} | For the log configuration, enter the permissions that will be granted to administrator accounts associated with this access profile. | none |
| ms365 {none \| read \| read-write} | For the Microsoft 365 configuration, enter the permissions that will be granted to administrator accounts associated with this access profile. | none |
| others {none \| read \| read-write} | For the rest of the configurations except policy, block-safe-list, and quarantine, enter the permissions that will be granted to administrator accounts associated with this access profile. | none |
| personal-quarantine {none \| read \| read-write} | For personal quarantine, enter the permissions that will be granted to administrator accounts associated with this access profile. | none |
| policy {none \| read \| read-write} | For the policy configuration, enter the permissions that will be granted to administrator accounts associated with this access profile. | none |
| privilege-level {high \| low \| medium} | Set the access profile's privilege level.<br>Any administrators assigned a `low` privilege level cannot run `diagnose` or `config system` commands. | medium |
| queue {none \| read \| read-write} | For the queue configuration, enter the permissions that will be granted to administrator accounts associated with this access profile. | none |
| system {none \| read \| read-write} | For system settings, enter the permissions that will be granted to administrator accounts associated with this access profile. | none |
| system-diagnostics {enable \| disable} | Enable or disable permission to run system diagnostic commands. | enable |
| system-quarantine {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 on page 256

# 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> on page 257
      set access-profile <profile_name> on page 257
      set auth-strategy {ldap | local | local-plus-radius | pki | radius} on page
          257
      set is-system-domain {no | yes} on page 257
      set language <lang_str> on page 257
      set ldap-profile <profile_name> on page 257
      set password <password_str> on page 257
      set pkiuser <pkiuser_str> on page 258
      set radius-permission-check {enable | disable} on page 258
      set radius-profile <profile_int> on page 258
      set radius-subtype-id <subtype_int>] on page 258
      set radius-vendor-id <vendor_int> on page 258
      set sshkey <key_str> on page 258
      set status {enable | disable} on page 258
      set theme on page 258
      set theme <theme_str> on page 258
      set trusthosts <host_ipv4mask> on page 258
      set webmode (basic | advanced) on page 258
end
```

| Variable | Description | Default |
|---|---|---|
| <name_str> | Enter the name of the administrator account. | |
| access-profile <profile_name> | Enter the name of an access profile that determines which functional areas the administrator account may view or affect. | |
| auth-strategy {ldap \| local \| local-plus-radius \| pki \| radius} | Select the local or remote type of authentication that the administrator will be able to use:<br>`ldap`<br>`local`<br>`radius`<br>`radius-plus-local`<br>`pki` | local |
| is-system-domain {no \| yes} | Enter `yes` to indicate that the administrator account may view all settings on the FortiMail unit. | yes |
| language <lang_str> | Enter this administrator account's preference for the display language of the web-based manager. Available languages vary by whether or not you have installed additional language resource files.<br>To view a list of languages, enter a question mark ( `?` ). | english |
| ldap-profile <profile_name> | If `auth-strategy` is `ldap`, enter the LDAP profile you want to use. | |
| password <password_str> | If `auth-strategy` is `local` or `radius-plus-local`, enter the password for the administrator account. | |

| Variable | Description | Default |
|---|---|---|
| | Caution: Do not enter a FortiMail administrator password less than six characters long. For better security, enter a longer password with a complex combination of characters and numbers, and change the password regularly. Failure to provide a strong password could compromise the security of your FortiMail unit. | |
| pkiuser <pkiuser_str> | If `auth-strategy` is `pki`, enter the name of a PKI user.<br>Whether the administrator is required to log in only with a valid personal certificate or password-style authentication fallback is allowed varies by your configuration of pki-mode {enable \| disable} on page 290. | |
| radius-permission-check {enable \| disable} | If `auth-strategy` is `local` or `radius-plus-local`, enable to query the RADIUS server for the permissions attribute. | disable |
| radius-profile <profile_int> | If `auth-strategy` is `local` or `radius-plus-local`, enter the index number of a RADIUS authentication profile. | |
| radius-subtype-id <subtype_int>] | If `auth-strategy` is `local` or `radius-plus-local`, and `radius-permission-check` is `enable`, enter the RADIUS subtype identifier. | 0 |
| radius-vendor-id <vendor_int> | If `auth-strategy` is `local` or `radius-plus-local`, and `radius-permission-check` is `enable`, enter the RADIUS vendor identifier. | 0 |
| sshkey <key_str> | Enter the SSH key string surrounded in single straight quotes ( ' ).<br>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. | |
| status {enable \| disable} | Enable to activate the admin user. | disable |
| theme | Enter the system admin GUI theme. | |
| theme <theme_str> | Enter this administrator account's preference for the display theme when logging in. | |
| trusthosts <host_ipv4mask> | Enter one to three IP addresses and netmasks from which the administrator can log in to the FortiMail unit. Separate each IP address and netmask pair with a comma ( , ).<br>To allow the administrator to authenticate from any IP address, enter `0.0.0.0/0.0.0.0`. | 0.0.0.0/0.0.0.0 |
| webmode (basic \| advanced) | Enter which display mode will initially appear when the administrator logs in to the web-based manager.<br>The administrator may switch the display mode during their session; this affects only the initial state of the display. | basic |

## Related topics

sensitive data on page 253

# system advanced-management

Use this command to control advanced management features.

The configuration of advanced management options is license based. This command is only available with a valid purchased advanced management license from FortiGuard.

Certain subcommands are only available as part of the MTA advanced control feature. See `mta-adv-ctrl-status` under system global on page 287

## Syntax

```
config system advanced-management
   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 |
|---|---|---|
| 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 intra domain protection. | disable |
| 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

report mailbox

system domain-group

system ha

# system appearance

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

## Syntax

```
config system appearance
   set admin-sso-login-option {normal | sso-only}
   set comment <string>
   set customized-login-status {enable | disable} on page 260
   set fallback-charset <language_code> on page 260
   set login-page-language <lang_str> on page 260
   set login-page-theme on page 260
   set product <product-name_str> on page 260
   set webmail-help-status {enable | disable) on page 260
   set webmail-help-url <url_str> on page 260
   set webmail-lang <language_str> on page 260
   set webmail-login <login_str> on page 261
   set webmail-login-hint <login_hint_str> on page 261
   set webmail-sort-option {order-received | time-received}
   set webmail-sso-login-option {normal | sso-only}
   set webmail-theme {IndigoDarkBlue | RedGrey | Standard} on page 261
   set webmail-theme-status {enable | disable} on page 261
end
```

| Variable | Description | Default |
|---|---|---|
| admin-sso-login-option {normal \| sso-only} | Define administrator SSO login handling:<br>• `normal`: Require both SSO and username/password.<br>• `sso-only`: Require SSO only. | normal |
| comment <string> | Optional comment for the system appearance. | |
| 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 <language_code> | Enter the fallback charset for non RFC 2047 compliant message. | english |
| login-page-language <lang_str> | Enter the default language for the display of the login page of the web manager.<br>To view a list of languages, enter a question mark ( `?` ).<br>Note that the setting only affect the login page, not the entire web-based manager. | english |
| login-page-theme | Enter the default display theme of the login page. | |
| product <product-name_str> | Enter the text that will precede 'Administrator Login' on the login page of the web-based manager. | FortiMail |
| webmail-help-status {enable \| disable) | Enable to display the help button in the webmail interface. The default help contents are provided by Fortinet. | enable |
| webmail-help-url <url_str> | If you want to provide your own help to the webmail users, you can enter the URL of the help file. | |
| webmail-lang <language_str> | Enter the name of the language in English, such as `'French'`, that will be used when an email user initially logs in to FortiMail webmail/per-recipient quarantine. | English |

| Variable | Description | Default |
|---|---|---|
| | The email user may switch the display language in their preferences; this affects only the initial state of the display.<br>Available languages vary by whether or not you have installed additional language resource files. | |
| webmail-login <login_str> | Enter a word or phrase that will appears on top of the webmail login page, such as Webmail Login. | Login |
| webmail-login-hint <login_hint_str> | Enter a hint for the user name, such as Your Email Address. This hint will apprear as a mouse-over display on the login name field. | address |
| webmail-sort-option {order-received \| time-received} | Define the email sorting option on webmail:<br>• `order-received`: Sorted by the order in which emails are delivered to the mailbox folder.<br>• `time-received`: Sorted by the time that emails are received by the mail server. | time-received |
| webmail-sso-login-option {normal \| sso-only} | Define webmail SSO login handling:<br>• `normal`: Require both SSO and username/password.<br>• `sso-only`: Require SSO only. | normal |
| webmail-theme {IndigoDarkBlue \| RedGrey \| Standard} | Select a theme for the webmail GUI. | RedGrey |
| webmail-theme-status {enable \| disable} | Enable or disable webmail theme change. | enable |

## Related topics

system geoip-override on page 286

# system backup-restore-mail

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

For the initial backup, whether manually or automatically initiated, the FortiMail unit will make a full backup. For subsequent backups, the FortiMail unit will make the number of incremental backups, 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> on page 262`. At that point, it will overwrite the oldest full backup.

For example, if `full <full-backups_int> on page 262` is 3 and `monthly-incremental-days on page 262` 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> on page 262
    set folder <path_str> on page 262
    set full <full-backups_int> on page 262
    set host <fortimail-fqdn_str> on page 262
    set hour-of-day <hours_int> on page 262
    set monthly-day-of-month on page 262
    set monthly-incremental-days on page 262
    set number-of-backups on page 262
    set port <port_int> on page 262
    set protocol {ext-usb | ext-usb-auto | iscsi_server | nfs | smb-winserver |
        ssh} on page 262
    set status {enable | disable} on page 263
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:<br>`/home/fortimail/mailboxbackups`<br>This field appears only if the backup media is an NFS server or SSH server. | FortiMail-mail-data-backup |
| full <full-backups_int> | Enter the total number of full backups to keep on the backup media. Valid values are between 1 and 10. | 3 |
| host <fortimail-fqdn_str> | If you want to restore all mailboxes from a backup labeled with the fully qualified domain name (FQDN) of a previous FQDN, or that of another FortiMail unit, enter the FQDN of the backup that you want to restore.<br>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.<br>For example, to make backups at 9 PM, enter `21`. | 23 |
| 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.<br>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:<br>`ext-usb`: An external hard drive connected to the FortiMail unit's USB port.<br>`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. | nfs |

| Variable | Description | Default |
|---|---|---|
| | `iscsi_server`: An Internet SCSI (Small Computer System Interface), also called iSCSI, server.<br>`nfs`: A network file system (NFS) server.<br>`smb/winserver`: A Windows-style file share.<br>`ssh`: A server that supports secure shell (SSH) connections.<br>Other available options vary by your choice of backup media. | |
| 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} on page 262` and, if applicable to the type of the media, configure a schedule in `encryption-key <key> on page 262` and `hour-of-day <hours_int> on page 262`<br>**Note**:You should enable backups/restoration **after** configuring the other options if a scheduled backup will occur before you configure `protocol {ext-usb \| ext-usb-auto \| iscsi_server \| nfs \| smb-winserver \| ssh} on page 262`. 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

system link-monitor on page 305

# system certificate ca

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

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

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

## Syntax

```
config system certificate ca
   edit <name_str> on page 263
      set certificate <cert_str> on page 263
end
```

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

## Related topics

system certificate crl on page 264
system certificate local on page 264
system certificate remote on page 265

# system certificate crl

Use this command to import certificate revocation lists.

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

## Syntax

```
config system certificate crl
   edit <name_str> on page 264
      set crl <cert_str> on page 264
end
```

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

## Related topics

system central-management
system certificate local on page 264
system certificate remote on page 265

# 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 <name_str> on page 265
      set password on page 265
      set private-key on page 265
      set certificate <cert_str> on page 265
      set csr <csr_str> on page 265
      set comments <comment_str> on page 265
end
```

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

## Related topics

system central-management

system certificate crl on page 264

system certificate remote on page 265

# system certificate remote

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

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

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

## Syntax

```
config system certificate remote
   edit <name_str> on page 266
      set certificate <cert_str> on page 266
end
```

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

## Related topics

system central-management

system certificate crl on page 264

system certificate local on page 264

# 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 Security Fabric member.

## Syntax

```
config system csf
   set configuration-sync {local | sync}
   set group-name <string>
   set group-password <password>
   set management-ip <string>
   set management-port <integer>
   set status {enable | disable}
   set upstream-ip <string>
   set upstream-port <integer>
end
```

| Variable | Description | Default |
|---|---|---|
| configuration-sync {local \| sync} | Configuration synchronization mode. | local |
| group-name <string> | Security Fabric group name. | |
| group-password <password> | Security Fabric group name password. | |
| management-ip <string> | Management IP address of the unit to join the Security Fabric. | |
| management-port <integer> | Management port number of the unit to join the Security Fabric. Set the value between 1-65535. | 443 |
| status {enable \| disable} | Enable or disable Security Fabric configuration. | enable |
| upstream-ip <string> | IP address of upstream. | 172.20.141.151 |
| upstream-port <integer> | Upstream port number. | 8013 |

# 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> on page 268
      config domain
         edit domain <domain_str> on page 268\
            set ipmode {auto | bind | static} on page 268
            set interface <interface_str> on page 268
            set ip <host_ipv4> on page 268
            set status {enable | disable} on page 268
            set type {custom | dynamic | static} on page 268
      set password <password_str> on page 268
```

```
        set timeout <time_int> on page 268
        set username <username_str> on page 268
    end
```

| Variable | Description | Default |
|---|---|---|
| <ddns-service_str> | Enter one of the following DDNS update servers:<br>• members.dhs.org<br>• dipdnsserver.dipdns.com<br>• www.dnsart.com<br>• members.dyndns.org<br>• www.dyns.net<br>• ip.todayisp.com<br>• ods.org<br>• rh.tzo.com<br>• ph001.oray.net<br>**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:<br>`auto`: Automatically detect the public IP address of the FortiMail unit and use that as the IP address to which `domain <domain_str> on page 268` will resolve.<br>`bind`: Use the IP address of a specific network interface as the IP address to which `domain <domain_str> on page 268` will resolve. Also configure `interface <interface_str> on page 268`.<br>`static`: Use the public IP address to which `domain <domain_str> on page 268` will resolve. Also configure `ip <host_ipv4> on page 268`. | 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> on page 268` will resolve. | |
| ip <host_ipv4> | Enter the public IP address to which `domain <domain_str> on page 268` 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 on page 272

# 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} on page 269
   set incoming-body-content <disclaimer_str> on page 269
   set incoming-body-content-html on page 269
   set incoming-body-location on page 269
   set incoming-body-status {enable | disable} on page 270
   set incoming-external-email-only {enable | disable}
   set incoming-header-insertion-name on page 270
   set incoming-header-insertion-value on page 270
   set incoming-header-status {enable | disable} on page 270
   set incoming-subject-tagging-status {enable | disable}
   set incoming-subject-tagging-value <string>
   set outgoing-body-content <disclaimer_str> on page 270
   set outgoing-body-content-html on page 270
   set outgoing-body-location on page 270
   set outgoing-body-status {enable | disable} on page 270
   set outgoing-header-insertion-name
   set outgoing-header-insertion-value
   set outgoing-header-status {enable | disable} on page 270
   set outgoing-subject-tagging-status {enable | disable}
   set outgoing-subject-tagging-value <string>
end
```

| Variable | Description | Default |
|---|---|---|
| exclude-status {enable \| disable} | If you do not want to insert disclaimers to the email messages from certain senders or to certain recipients, you can enable this option. For information about how to configure the disclaimer exclusion list, see system disclaimer-exclude on page 271. | disable |
| incoming-body-content <disclaimer_str> | Enter the text that comprises the disclaimer message that appends to the message body of each incoming email. | |
| incoming-body-content-html | Enter the text that comprises the content of the HTML incoming disclaimer in the message body. | |
| incoming-body-location | Enter an incoming disclaimer at the beginning or end of a message body. | |

| Variable | Description | Default |
|---|---|---|
| incoming-body-status {enable \| disable} | Enable to append a disclaimer to the message body of each incoming email. Also configure incoming-body-content <disclaimer_str> on page 269. | disable |
| incoming-external-email-only {enable \| disable} | Enable to insert incoming disclaimer warning of any emails that come from outside the organization (for external email only). | disable |
| incoming-header-insertion-name | Enter the name of the header to be inserted for incoming disclaimer. | |
| incoming-header-insertion-value | Enter the value of the header to be inserted for incoming disclaimer. | |
| incoming-header-status {enable \| disable} | Enable to insert a disclaimer to the message header of each incoming email. Also configure system disclaimer on page 269. | disable |
| incoming-subject-tagging-status {enable \| disable} | Enable to insert subject tag for incoming email. | |
| incoming-subject-tagging-value <string> | Enter the subject tag text that is prepended to the subject line of incoming email. | |
| outgoing-body-content <disclaimer_str> | Enter the text that comprises the disclaimer message that appends to the message body of each outgoing email. | |
| outgoing-body-content-html | Enter the content of html outgoing disclaimer in the message body. | |
| outgoing-body-location | Enter the outgoing disclaimer at the beginning or ending of the message body. | |
| outgoing-body-status {enable \| disable} | Enable to append a disclaimer to the message body of each outgoing email. Also configure outgoing-body-content <disclaimer_str> on page 270. | disable |
| outgoing-header-insertion-name | Enter the name of the header to be inserted for outgoing disclaimer. | |
| outgoing-header-insertion-value | Enter the value of the header to be inserted for outgoing disclaimer. | |
| outgoing-header-status {enable \| disable} | Enable to insert a disclaimer to the message header of each outgoing email. Also configure outgoing-body-content <disclaimer_str> on page 270. | disable |
| outgoing-subject-tagging-status {enable \| disable} | Enable to insert subject tag for outgoing email. | |

| Variable | Description | Default |
|---|---|---|
| outgoing-subject-tagging-value <string> | Enter the subject tag text that is prepended to the subject line of outgoing email. | |

## Related topics

system disclaimer-exclude on page 271

# 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 <id> on page 271
      set recipient-pattern <string> on page 271
      set sender-pattern <string> on page 271
      set source-ip <ipv4mask>
end
```

| Variable | Description | Default |
|---|---|---|
| <id> | Enter a table ID. | |
| recipient-pattern <string> | 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 <string> | 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 <ipv4mask> | Define the source IP address and netmask to exclude from disclaimers. | 0.0.0.0/0 |

## Related topics

system disclaimer on page 269

# 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} on page 272
   set cache-min-ttl <time-in-seconds> on page 272
   set primary <ipv4_address> on page 272
   set protected-domain-dns-servers <ipv4_address> on page 272
   set protected-domain-dns-state {enable | disable} on page 272
   set ptr-query-option {enable | disable| public-ip-only} on page 273
   set secondary <dns_ipv4> on page 273
   set truncate-handling {disable | tcp-retry} on page 273
end
```

| Variable | Description | Default |
|---|---|---|
| cache {enable \| disable} | Enable to cache DNS query results to improve performance.<br>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.<br>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 |
| protected-domain-dns-state {enable \| disable} | Either enable or disable the protected domain DNS servers. | disable |

| Variable | Description | Default |
|---|---|---|
| ptr-query-option {enable \| disable\| public-ip-only} | Enable to perform reverse DNS lookups on both private network IP addresses and public IP addresses.<br>However, PTR queries may cause delays when the DNS server has no response. In this situation, you may choose to disable the querying.<br>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 on page 267

# 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> on page 273
      set domain <string> on page 273
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 on page 274

# system encryption ibe

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

## 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} on page 275
   set expire-alert <days_int>
   set expire-emails <days_int> on page 275
   set expire-inactivity <days_int> on page 275
   set expire-passwd-reset <hours_int> on page 275
   set expire-registration <days_int> on page 275
   set read-notification {enable | disable} on page 275
   set secure-compose {enable | disable} on page 275
   set secure-reply {enable | disable} on page 275
   set secure-forward {enable | disable} on page 275
   set secure-token-ttl <minutes>
   set service-name <name_str> on page 276
   set sms-account-id <id>
   set sms-auth-key <key>
   set sms-from-number <number>
   set sms-provider <provider>
   set status {enable | disable} on page 276
   set two-factor-auth-max-attempt <attempts_int>
   set two-factor-auth-method {email | sms}
   set unread-days on page 276
   set unread-notif-rcpt on page 276
   set unread-notif-sender on page 276
   set unread-notification {enable | disable} on page 276
   set url-about <url_str> on page 276
   set url-base <url_str> on page 276
   set url-custom-user-control <url_str> on page 276
   set url-forgot-pwd <psw_str> on page 277
   set url-help <url_str> on page 277
end
```

| Variable | Description | Default |
|---|---|---|
| account-notification {activation deletion expiration registration-confirmation reset-confirmation} | Enter the types of account notifications you wish to be sent to users.<br>Optionally, for multiple account notifications, separate each entry with a space. | activation expiration |

| Variable | Description | Default |
|---|---|---|
| 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.<br>Also configure `url-custom-user-control` and `url-forgot-pwd`. | 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.<br>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.<br>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.<br>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 |
| 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.<br>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 |

| Variable | Description | Default |
|---|---|---|
| secure-token-ttl <minutes> | Enter the secure token timeout value in minutes. Set the value between 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 <id> | Enter the account or service plan ID provided by your SMS provider. | |
| sms-auth-key <key> | 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 <provider> | 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` is set to either `token` or `two-factor`.<br>Enter the verification method for two-factor authentication: email or SMS. | email |
| unread-days | **Note**: This option is only available when `unread-notification` is set to `enable`.<br>Enter the unread notification days. | 14 |
| unread-notif-rcpt | **Note**: This option is only available when `unread-notification` is set to `enable`.<br>Enable to send the unread notification to the recipient. | disable |
| unread-notif-sender | **Note**: This option is only available when `unread-notification` is set to `enable`.<br>Enable to send the unread notification to the sender. | disable |
| unread-notification {enable \| disable} | Enable to send the unread notification if the message remains unread for 14 days by default. | disable |
| url-about <url_str> | You can create a file about the FortiMail IBE encryption and enter the URL for the file. The mail recipient can click the “About” link from the secure mail notification to view the file.<br>If you leave this option empty, a link for a default file about the FortiMail IBE encryption will be added to the secure mail notification. | |
| url-base <url_str> | Enter the FortiMail unit URL, for example, https://192.168.100.20, where a mail recipient can register or authenticate to access the secured mail. | |
| url-custom-user-control <url_str> | Enter the URL where you can check for user existence. This command appears after you enable `custom-user-control-status`. | |

| Variable | Description | Default |
|---|---|---|
| url-forgot-pwd <psw_str> | Enter the URL where users get authenticated. This command appears after you enable `custom-user-control-status`. | |
| url-help <url_str> | You can create a help file on how to access the FortiMail secure email and enter the URL for the file. The mail recipient can click the “Help” link from the secure mail notification to view the file.<br>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 on page 277

# 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 on it under the *User* > *IBE User* > *IBE Domain* tab.

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 216”.

## Syntax

```
config system encryption ibe-auth
   edit <id> on page 277
      set domain-pattern <string> on page 277
      set ldap-profile <profile_name> on page 278
      set status {enable | disable} on page 278
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.<br>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. | |

| Variable | Description | Default |
|---|---|---|
| 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 on page 274

# 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> on page 279
   set override-server-status {enable | disable} on page 279
   set push-update-override-address <virtual-ip_ipv4> on page 279
   set push-update-override-port <port_int> on page 279
   set push-update-override-status {enable | disable} on page 279
   set push-update-status {enable | disable} on page 279
   set scheduled-update-day <day_int> on page 279
   set scheduled-update-frequency {daily | every | weekly} on page 279
   set scheduled-update-status {enable | disable} on page 279
   set scheduled-update-time <time_str> on page 279
   set tunneling-address <host_ipv4> on page 279
   set tunneling-password <password_str> on page 279
   set <document id> on page 254
   set tunneling-status {enable | disable} on page 279
   set tunneling-username <username_str> on page 280
   set virus-db {default | extended | extreme} on page 280
   set virus-outbreak {diable | enable | enable-with-defer} on page 280
   set virus-outbreak-protection-period <minutes> on page 280
end
```

| Variable | Description | Default |
|---|---|---|
| override-server-address <virtual-ip_ipv4> | If `override-server-status` is `enable`, enter the IP address of the public or private FortiGuard Distribution Server (FDS) that overrides the default FDS to which the FortiMail unit connects for updates. | |
| override-server-status {enable \| disable} | Enable to override the default FDS to which the FortiMail unit connects for updates. | disable |
| push-update-override-address <virtual-ip_ipv4> | If `push-update-override-status` is `enable`, enter the public IP address that will forward push updates to the FortiMail unit. Usually, this is a virtual IP address on the external interface of a NAT device such as a firewall or router. | |
| push-update-override-port <port_int> | If `push-update-override-status` is `enable`, enter the port number that will forward push updates to UDP port 9443 the FortiMail unit. Usually, this is a port forward on the external interface of a NAT device such as a firewall or router. | |
| push-update-override-status {enable \| disable} | Enable to override the default IP. | disable |
| push-update-status {enable \| disable} | Enable to allow the FortiMail unit to receive notifications of available updates, which trigger it to download FortiGuard Antivirus packages from the FDN. | disable |
| scheduled-update-day <day_int> | Enter the day of the week at which the FortiMail unit will request updates where the range is from 0-6 and 0 means Sunday and 6 means Saturday. | |
| scheduled-update-frequency {daily \| every \| weekly} | Enter the frequency at which the FortiMail unit will request updates. Also configure scheduled-update-day <day_int> on page 279 and scheduled-update-time <time_str> on page 279. | 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 <host_ipv4> | If `tunneling-status` is `enable`, enter the IP address of the web proxy. | |
| tunneling-password <password_str> | If `tunneling-status` is `enable`, enter the password of the account on the web proxy. | |
| tunneling-port <port_int> | If `tunneling-status` is `enable`, enter the TCP port number on which the web proxy listens. | |
| tunneling-status {enable \| disable} | Enable to tunnel update requests through a web proxy. | disable |

| Variable | Description | Default |
|---|---|---|
| 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:<br>• Default: The default FortiMail virus database contains most commonly seen viruses and should be sufficient enough for regular antivirus protection.<br>For the current release, FortiMail VM00 model supports the default virus database only.<br>• Extended: Some high-end FortiMail models support the usage of an extended virus database, which contains viruses that are not active any more.<br>For the current release, FortiMail VM01/VM02/200F/400F models support both the default and extended virus databases.<br>• 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.<br>For the current release, FortiMail VM04/900F and above models support all three types of virus databases. | default |
| virus-outbreak {diable \| enable \| enable-with-defer} | When a virus outbreak occurs, the FortiGuard antivirus database may need some time to get updated. Therefore, you can choose to defer the delivery of the suspicious email messages and scan them for the second time:<br>• Disable: Do not query FortiGuard antivirus service.<br>• Enable: Query FortiGuard antivirus service.<br>• Enable with Defer: If the first query returns no results, defer the email for the specified time and do the second query. | enable-with-defer |
| virus-outbreak-protection-period <minutes> | If you specify Enable with Defer in the above field, specify how many minutes later a second query will be done. | 20 |

## Related topics

system fortiguard antispam on page 280
update on page 374

# system fortiguard antispam

Use this command to configure how the FortiMail unit will connect to the FortiGuard servers to query for antispam signatures. Unlike the antivirus updates, FortiMail cannot query FortiGuard antispam service via a web proxy. If there is a web proxy before FortiMail, you have to use a FortiManager unit locally as an override server.

## Syntax

```
config system fortiguard antispam
```

```
    set cache-mpercent <percentage_int> on page 281
    set cache-status {enable | disable} on page 281
    set cache ttl <ttl_int> on page 281
    set hostname {<fqdn_str> | <host_ipv4>} on page 281
    set outbreak-protection-level {disable | high | low | medium} on page 281
    set outbreak-protection-period <minutes> on page 281
    set port {443 | 53 | 8888} on page 281
    set protocol {udp | https} on page 281
    set query-timeout <timeout_int> on page 281
    set action-rbl <action-profile_name> on page 174
    set server-override-ip <ipv4> on page 282
    set server-override-status {enable | disable} on page 282
    set status {enable | disable} on page 282
    set threshold-ip-connect <integer> on page 282
    set uri-redirect-lookup {enable | disable} on page 282
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. | enable |
| cache ttl <ttl_ int> | Enter the TTL in seconds for cache entries. | 300 |
| hostname {<fqdn_str> \| <host_ipv4>} | Enter an IP address or a fully qualified domain name (FQDN) to override the default FortiGuard Antispam query server. | antispam.fortigate.com |
| outbreak-protection-level {disable \| high \| low \| medium} | Specify a spam outbreak protection level. Higher levels mean stricter filtering.<br>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 URI filter) returns no result. After the specified time interval, FortiMail will query the FortiGuard server for the second time. This provides an opportunity for the FortiGuard antispam service to update its database in cases a spam outbreak occurs.<br>Conversely, in order to reduce the types of email to be deferred for outbreak, set this command to `low`. | medium |
| outbreak-protection-period <minutes> | 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. | |
| query-timeout <timeout_int> | Enter the timeout value for the FortiMail unit to query the FortiGuard Antispam query server. | 7 |

| Variable | Description | Default |
|---|---|---|
| server-location | Limit the FortiGuard servers to certain locations. | |
| server-override-ip <ipv4> | If `server-override-status` is `enable`, enter the IP address of the public or private FortiGuard Antispam query server that overrides the default query server to which the FortiMail unit connects. | |
| 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 |
| status {enable \| disable} | Enable to query to the FortiGuard Distribution Network (FDN) for FortiGuard Antispam ratings.<br>This option must be enabled for antispam profiles where the FortiGuard Antispam scan is enabled to have an effect. | enable |
| threshold-ip-connect <integer> | When you configure the FortiGuard IP reputation check under Sender Reputation in a session profile, if you choose the "When client connect" option, that means you want the FortiGuard Antispam Service to determine if the IP address of the SMTP server is blocklisted during the connection phase.<br>FortiGuard categorizes the blocklisted IP addresses into three levels -- level 3 has bad reputation; level 2 has worse reputation; and level 1 has the worst reputation. To help prevent false positives, you can choose to this command to specify which level to block.<br>*<integer>* is the level number: 1, 2, or 3. The default setting is 3, which means all levels will be blocked. If you want to block level 1 and level 2 but not level 3, you set it to 2. | 3 |
| uri-redirect-lookup {enable \| disable} | If an email contains a shortened URI that redirects to another URI, the FortiMail unit is able to send a request to the shortened URI to get the redirected URI and scan it against the FortiGuard AntiSpam database. By default, this function is enabled. To use it, you need to open your HTTP port to allow the FortiMail unit to send request for scanning the redirected URI. | enable |

## Related topics

system fortiguard antivirus on page 278
update on page 374

# system fortiguard url-protection

Use this command to configure content disarm and reconstruction (CDR) URL 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-url-base <string>
   set malformed-html-tag-content-action {remove | rewrite}
   set neutralize-category {all | default | phishing | unrated}
   set remove-category {all | default | phishing | unrated}
   set rewrite-category {all | default | phishing | unrated}
   set rewrite-url-base <string>
   set sandbox-click-action {allow-with-confirmation | block | submit-only}
   set sandbox-status {enable | disable}
   set sandbox-timeout <integer>
   set sandbox-timeout-action {allow | allow-with-confirmation | block}
end
```

| Variable | Description | Default |
|---|---|---|
| click-action {allow-with-confirmation \| block} | Set the FortiSandbox scan action for the click handling category. | block |
| click-category {all \| default \| phishing \| unrated} | Set the URL filter category profile used to authorize URLs on click. | default |
| isolator-category {all \| default \| phishing \| unrated} | Set the URL filter category profile used to identify URLs to be rewritten by FortiIsolator. | unrated |
| isolator-url-base <string> | Define the rewrite URL base. Enter the prefix `https://` followed by the FortiIsolator FQDN or IP address. | |
| malformed-html-tag-content-action {remove \| rewrite} | Set the malformed HTML tag content action: remove or rewrite URLs that are not exempted. | remove |
| neutralize-category {all \| default \| phishing \| unrated} | Set the URL filter category profile used to identify URLs to neutralize. | unrated |
| remove-category {all \| | Set the URL filter category profile used to identify URLs to remove. | default |

| Variable | Description | Default |
|---|---|---|
| default \| phishing \| unrated} | | |
| rewrite-category {all \| default \| phishing \| unrated} | Set the URL filter category profile used to identify URLs to rewrite. | unrated |
| rewrite-url-base <string> | Define the rewrite URL base. Enter the prefix `https://` followed by the FortiMail FQDN or IP address. | |
| sandbox-click-action {allow-with-confirmation \| block \| submit-only} | Set the FortiSandbox click action:<br>• `allow-with-confirmation`: Allow access with a warning.<br>• `block`: Block access.<br>• `submit-only`: Allows access while sending the URLs for scanning. | allow-with-confirmation |
| sandbox-status {enable \| disable} | Enable or disable FortiSandbox scanning. | disable |
| sandbox-timeout <integer> | Specify how long (in seconds) you want to wait for FortiSandbox scan results before you take block, allow, or allow with confirmation actions. | 5 |
| sandbox-timeout-action {allow \| allow-with-confirmation \| block} | Set the FortiSandbox timeout action.<br>When URLs are sent to FortiSandbox for scanning, it may take a while to get the results back. It's recommended to specify how long you want to wait for the results (see sandbox-timeout <integer>) before an action is taken. | allow |

# 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 on page 285
```

```
      edit <table_value> on page 285
        set pattern <string> on page 285
      end
    config file-types on page 285
      edit {adobe-flash | archive | html | jar | javascript | pdf | msoffice-document |
          windows-executable}
        set status {enable | disable} on page 285
      end
    set admin-email <email_str> on page 285
    set bypass-one-time-url {enable | disable}
    set host <hostname_or_ip> on page 285
    set max-file-size <integer_value> on page 285
    set max-file-size-status {enable | disable} on page 285
    set max-uri-per-email on page 285
    set scan-mode {scan-and-wait | scan-only} on page 286
    set scan-order {antispam-content-sandbox | antispam-sandbox-content | sandbox-
        antispam-content} on page 286
    set scan-result-retention on page 286
    set scan-timeout on page 286
    set service-type {appliance | cloud | cloud-enhanced} on page 286
    set statistics-interval <minutes> on page 286
    set status {enable | disable} on page 286
    set uri-scan-category on page 286
    set uri-scan-email-selection on page 286
    set uri-scan-on-rating-error {enable | disable} on page 286
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. | |
| 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-uri-per-email | Maximum number of URIs per email to be scanned. Range between 1-12. | 3 |

| Variable | Description | Default |
|---|---|---|
| scan-mode {scan-and-wait \| scan-only} | `scan-and-wait` means to submit the suspicious email to FortiSandbox and wait for the results.<br>`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.<br>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.<br>Set the value between 1 to 30. | 5 |
| status {enable \| disable} | Either enable or disable the usage of the unit. | disable |
| uri-scan-category | Category of the URI to be scanned:<br>• Security-Risk<br>• all<br>• default<br>• phishing<br>• unrated | unrated |
| uri-scan-email-selection | Selection of email for URI scan. | |
| uri-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 URIs to FortiSandbox for scanning. Choosing not to upload those URIs may help improving the FortiSandbox performance. | disable |

# system geoip-override

Use this command to override the GeoIP lookup by manually specifying the geolocations of some IP addresses/IP ranges.

## Syntax

```
config system geoip-override
   set description on page 287
   set country-code on page 287
end
```

| Variable | Description | Default |
|---|---|---|
| description | Enter a description. | |
| country-code | Enter the two letter country code (for example US, CA). | |

# system global

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

## Syntax

```
config system global
   set admin-idle-timeout <timeout_int> on page 288
   set admin-lockout-duration on page 288
   set admin-lockout-threshold on page 288
   set admin-maintainer {enable | disable}
   set default-certificate <name_str> on page 288
   set dh-params <params_int> on page 288
   set disclaimer-per-domain {enable | disable} on page 288
   set disk-monitor {enable | disable} on page 288
   set email-migration-status {enable | disable} on page 288
   set hostname <host_str> on page 288
   set iscsi-initiator-name <name_str> on page 288
   set lcd-pin <pin_int> on page 288
   set lcd-protection {enable | disable} on page 289
   set ldap-server-sys-status {enable | disable} on page 289
   set ldap-sess-cache-state {enable | disable} on page 289
   set local-domain-name <name_str> on page 289
   set mailbox-service {enable | disable}
   set mailstat-service {enable | disable} on page 289
   set max-admin-per-domain <integer>
   set mta-adv-ctrl-status {enable | disable} on page 289
   set operation-mode {gateway | server | transparent} on page 289
   set pki-certificate-req {yes | no} on page 289
   set pki-mode {enable | disable} on page 290
   set port-http <port_int> on page 290
   set port-https <port_int> on page 290
   set port-ssh <port_int> on page 290
   set port-telnet <port_int> on page 290
   set post-login-banner {admin | ibe | webmail} on page 290
   set pre-login-banner admin on page 290
   set ssl-versions {ssl3 tls1_0 | tls1_1 | tls1_2 | tls1_3} on page 290
   set strong-crypto {enable | disable} on page 290
   set tftp {enable | disable} on page 291
```

```
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.<br>The maximum idle time out is 480 minutes (eight hours). To improve security, do not increase the idle timeout. | 5 |
| admin-lockout-duration | Enter the lockout duration in minutes after the failed login threshold is reached. | 3 |
| admin-lockout-threshold | 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.<br>Note that there is a limited time to complete this login.<br>If you attempt 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.<br>FortiMail units require a local server certificate that it can present when clients request secure connections. | factory |
| dh-params <params_int> | Enter the minimum size of Diffie-Hellman prime for SSH/HTTPS. | 1024 |
| disclaimer-per-domain {enable \| disable} | Enable to allow individualized disclaimers to be configured for each protected domain. | |
| disk-monitor {enable \| disable} | Enable to monitor the hard disk status of the FortiMail unit. If a problem is found, an alert email is sent to the administrator. | disable |
| email-migration-status {enable \| disable} | Enable the email migration from external server. | |
| hostname <host_str> | Enter the host name of the FortiMail unit. | Varies by model. |
| hsts-max-age <days> | Set the HTTP Strict Transport Security (HSTS) max-age. 0 means to disable. | 365 |
| iscsi-initiator-name <name_str> | Enter the FortiMail ISCSI client name used to communicate with the ISCSI server for centralized quarantine storage.<br>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.<br>The PIN is used only when `lcdprotection` is `enable`. | Encoded value varies. |

| Variable | Description | Default |
|---|---|---|
| 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. | |
| mailbox-service {enable \| disable} | **Note:** The mailbox service feature is license based. If you do not purchase the advanced management license, this feature is not available.<br>Enable the mailbox service.<br>After you enable this service, see report mailbox for information on configuring the mailbox service.<br>New options also appear in the GUI under *FortiView* > *Mail Statistics* > *Active Mailbox*. | |
| mailstat-service {enable \| disable} | Enable the mail statistic service.<br>After you enable this service, a new tab called Top User Statistics will appear under FortiView on the GUI. | disable |
| max-admin-per-domain <integer> | Set the maximum number of admins per domain. The valid range is 1 to 10. | 3 |
| mta-adv-ctrl-status {enable \| disable} | **Note:** The MTA advanced control feature is license based. If you do not purchase the advanced management license, this feature is not available.<br>Enable to configure advanced session-specific MTA settings (see profile session on page 235) and overwrite the global settings configured elsewhere. | enable |
| operation-mode {gateway \| server \| transparent} | **Note:** Only administrators with super admin privileges may change the FortiMail unit's operation mode.<br>Enter one of the following operation modes:<br>• `gateway`: The FortiMail unit acts as an email gateway or MTA, but does not host email accounts.<br>• `server`: The FortiMail unit acts as a standalone email server that hosts email accounts and acts as an MTA.<br>• `transparent`: The FortiMail unit acts as an email proxy. | gateway |
| pki-certificate-req {yes \| no} | If the administrator's web browser does not provide a valid personal certificate for PKI authentication, the FortiMail unit will fall back to standard user name and password-style authentication. To require valid certificates only and disallow password-style fallback, enter `yes`. To allow password-style fallback, enter `no`. | no |

| Variable | Description | Default |
|---|---|---|
| pki-mode {enable \| disable} | Enable to allow PKI authentication for FortiMail administrators. For more information, see user pki on page 330 and system admin on page 256.<br>Also configure `pki-certificate-req {yes \| no}` on page 289.<br>**Caution**: Before disabling PKI authentication, select another mode of authentication for FortiMail administrators and email users that are currently using PKI authentication. Failure to first select another authentication method before disabling PKI authentication will prevent them from being able to log in. | disable |
| 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} | Enable or disable the legal disclaimer.<br>`admin`: Select to display the disclaimer message **after** the administrator logs into the FortiMail web UI.<br>`webmail`: Select to display the disclaimer message after the user logs into the FortiMail webmail.<br>`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 web UI. | admin |
| ssl-versions {ssl3 tls1_0 \| tls1_1 \| tls1_2 \| tls1_3} | Specify which SSL/TLS versions you want to support for the HTTPS and SMTP access to FortiMail. Currently, TLS 1.0, TLS 1.1, TLS 1.2, and TLS 1.3 are supported.<br>In 6.0.0 release, `strong-crypto` is enabled and TLS 1.0 is disabled by default. Because some old versions of email clients (for example, MS Outlook 2007 and older) and MTAs only support TLS 1.0, they may have issues connecting to FortiMail. To fix the issue, disable `strong-crypto` and add TLS 1.0 support.<br>Starting from 6.0.1 release, both `strong-crypto` and TLS 1.0 are enabled by default.<br>Starting from 6.2.0, when strong-crypto is enabled, TLS 1.0 is disabled.<br>When `strong-crypto` is enabled, SSL 3.0 is only supported in 5.4 releases, not in 6.0 and 6.2 releases. | ssl3 tls1_0, tls1_1, tls1_2 tls1_3 |
| strong-crypto {enable \| disable} | Enable to use strong encryption and only allow strong ciphers (AES) and digest (SHA1) for HTTPS/SSH admin access.<br>When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta) and higher.<br>Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption. | enable |

| Variable | Description | Default |
|---|---|---|
| tftp {enable \| disable} | Enable to allow use of TFTP in FIPS mode. | enable |

## Related topics

config domain-setting on page 105

# system ha

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

## Syntax

```
config system ha
   config interface
      edit <interface_name> on page 292
         set status {enable | disable} on page 125
         set heartbeat-status <disable | primary | secondary} on page 292
         set peer-ip <ipv4_netmask> on page 293
         set peer-ip6 <ipv6_netmask> on page 293
         set port-monitor {enable | disable} on page 293
         set virtual-ip <ipv4_netmask> on page 293
         set virtual-ip6 <ipv6_netmask> on page 293
   config service
      edit <remote-smtp> on page 293
         set check-interval <integer> on page 293
         set check-timeout <integer> on page 293
         set ip <ip_addr> on page 294
         set port <port_num> on page 294
         set retries <integer> on page 294
         set status {enable | disable} on page 294
      edit <remote-imap> on page 294
         set check-interval <integer> on page 294
         set check-timeout <integer> on page 294
         set ip <ip_addr> on page 294
         set port <port_num> on page 294
         set retries <integer> on page 294
         set status {enable | disable} on page 294
      edit <remote-pop> on page 294
         set check-interval <integer> on page 294
         set check-timeout <integer> on page 294
         set ip <ip_addr> on page 294
         set port <port_num> on page 294
         set retries <integer> on page 294
         set status {enable | disable} on page 294
      edit <remote-http> on page 294
         set check-interval <integer> on page 294
```

```
      set check-timeout <integer> on page 294
      set ip <ip_addr> on page 294
      set port <port_num> on page 294
      set retries <integer> on page 294
      set status {enable | disable} on page 294
    edit <local-ports> on page 294
      set check-interval <integer> on page 295
      set retries <integer> on page 295
      set status {enable | disable} on page 295
    edit <local-hd> on page 295
      set check-interval <integer> on page 295
      set retries <integer> on page 295
      set status {enable | disable} on page 295
  set system ha
  set config-peer-ip <ip_addr> on page 295
  set failover <interface_str> {add | bridge | ignore | set}<address_ipv4mask>
      on page 295
  set hard-drives-check {enable | disable} on page 296
  set hb-base-port <interface_int> on page 296
  set hb-lost-threshold on page 296
  set heartbeat-1-interface <interface_int> on page 297
  set heartbeat-1-ip <local_ipv4mask> on page 297
  set heartbeat-1-peer <primary-peer_ipv4> on page 297
  set heartbeat-2-interface <interface_str> on page 297
  set heartbeat-2-ip <secondary-local_ipv4mask> on page 297
  set heartbeat-2-peer <secondary-peer_ipv4> on page 297
  set mail-data-sync {enable | disable} on page 298
  set mailqueue-data-sync {enable | disable} on page 298
  set mode {config-primary | config-secondary | primary | off | secondary} on
      page 298
  set on-failure {off | restore-role | become-secondary} on page 299
  set password <password_str> on page 299
  set remote-services-as-heartbeat {enable | disable} on page 300
end
```

| Variable | Description | Default |
|---|---|---|
| <interface_name> | Enter the interface name of which you want to configure the virtual IP. | |
| action-on-primary {ignore-vip \| use-vip} | Select whether and how to configure the IP addresses and netmasks of the primary FortiMail unit:<br>• `ignore-vip`: Do not change the network interface configuration on failover, and do not monitor.<br>• `use-vip`: Add the specified virtual IP address and netmask to the network interface on failover. Normally, you will configure your network (MX records, firewall policies, routing and so on) so that clients and mail services use the virtual IP address. Both originating and reply traffic uses the virtual IP address. This option results in the network interface having two IP addresses: the actual and the virtual. | ignore-vip |
| heartbeat-status <disable \| primary \| secondary} | Specify if this interface will be used for HA heartbeat and synchronization.<br>• `disable`: Do not use this interface for HA heartbeat and synchronization.<br>• `primary`: Select the primary network interface for heartbeat and synchronization traffic. | |

| Variable | Description | Default |
|---|---|---|
| | This network interface must be connected directly or through a switch to the ***Primary heartbeat*** network interface of other members in the HA group.<br>• `secondary`: Select the secondary network interface for heartbeat and synchronization traffic.<br>The secondary heartbeat interface is the backup heartbeat link between the units in the HA group. If the primary heartbeat link is functioning, the secondary heartbeat link is used for the HA heartbeat. If the primary heartbeat link fails, the secondary link is used for the HA heartbeat and for HA synchronization.<br>This network interface must be connected directly or through a switch to the ***Secondary heartbeat*** network interfaces of other members in the HA group.<br>**Caution**: Using the same network interface for both HA synchronization/heartbeat traffic and other network traffic could result in issues with heartbeat and synchronization during times of high traffic load, and is not recommended.<br>**Note**: In general, you should isolate the network interfaces that are used for heartbeat traffic from your overall network. Heartbeat and synchronization packets contain sensitive configuration information, are latency-sensitive, and can consume considerable network bandwidth. | |
| peer-ip <ipv4_ netmask> | Enter the IP address of the matching heartbeat network interface of the other member of the HA group.<br>For example, if you are configuring the primary unit's primary heartbeat network interface, enter the IP address of the secondary unit's primary heartbeat network interface.<br>Similarly, for the secondary heartbeat network interface, enter the IP address of the other unit's secondary heartbeat network interface.<br>This option appears only for active-passive HA. | |
| peer-ip6 <ipv6_ netmask> | Enter the peer IPv6 address in the active-passive HA group. | |
| port-monitor {enable \| disable} | Enable to monitor a network interface for failure. If the port fails, the primary unit will trigger a failover.<br>This option applies only if local network interface monitoring is enabled. | |
| virtual-ip <ipv4_ netmask> | Enter the virtual IP address and netmask for this interface.<br>This option is available only if `status {enable \| disable} on page 125` is set. | 0.0.0.0/0 |
| virtual-ip6 <ipv6_ netmask> | Enter the virtual IPv6 address and netmask for this interface.<br>This option is available only if `status {enable \| disable} on page 125` is set. | 0.0.0.0/0 |
| <remote-smtp> | Enter to configure the remote SMTP service monitoring. | |
| check-interval <integer> | Enter the time interval between service checks in seconds. | 120 |
| check-timeout <integer> | Enter the timeout for remote service check in seconds. | 30 |

| Variable | Description | Default |
|---|---|---|
| ip <ip_addr> | Enter the SMTP server IP address for service check. | 0.0.0.0 |
| port <port_num> | Enter the SMTP server port number for service check. | 25 |
| retries <integer> | Enter the number of attempts to try before considering the SMTP server a failure. | 3 |
| status {enable \| disable} | Enable to start the remote SMTP service monitoring. | disable |
| <remote-imap> | Enter to configure the remote IMAP service monitoring. | |
| check-interval <integer> | Enter the time interval between service checks in seconds. | 120 |
| check-timeout <integer> | Enter the timeout for remote service check in seconds. | 30 |
| ip <ip_addr> | Enter the IMAP server IP address for service check. | 0.0.0.0 |
| port <port_num> | Enter the IMAP server port number for service check. | 143 |
| retries <integer> | Enter the number of attempts to try before considering the IMAP server a failure. | 3 |
| status {enable \| disable} | Enable to start the remote IMAP service monitoring. | disable |
| <remote-pop> | Enter to configure the remote POP service monitoring. | |
| check-interval <integer> | Enter the time interval between service checks in seconds. | 120 |
| check-timeout <integer> | Enter the timeout for remote service check in seconds. | 30 |
| ip <ip_addr> | Enter the POP server IP address for service check. | 0.0.0.0 |
| port <port_num> | Enter the POP server port number for service check. | 110 |
| retries <integer> | Enter the number of attempts to try before considering the POP server a failure. | 3 |
| status {enable \| disable} | Enable to start the remote POP service monitoring. | disable |
| <remote-http> | Enter to configure the remote HTTP service monitoring. | |
| check-interval <integer> | Enter the time interval between service checks in seconds. | 120 |
| check-timeout <integer> | Enter the timeout for remote service check in seconds. | 30 |
| ip <ip_addr> | Enter the HTTP server IP address for service check. | 0.0.0.0 |
| port <port_num> | Enter the HTTP server port number for service check. | 80 |
| retries <integer> | Enter the number of attempts to try before considering the HTTP server a failure. | 3 |
| status {enable \| disable} | Enable to start the remote HTTP service monitoring. | disable |
| <local-ports> | Enter to configure the local network interfaces service monitoring. | |

| Variable | Description | Default |
|---|---|---|
| check-interval <integer> | Enter the time interval between service checks in seconds. | 120 |
| retries <integer> | Enter the number of attempts to try before considering the local network interface a failure. | 3 |
| status {enable \| disable} | Enable to start the local network interface service monitoring. | disable |
| <local-hd> | Enter to configure the local hard drives service monitoring. | |
| check-interval <integer> | Enter the time interval between service checks in seconds. | 120 |
| retries <integer> | Enter the number of attempts to try before considering the hard drive a failure. | 3 |
| status {enable \| disable} | Enable to start the local hard drive service monitoring. | disable |
| config-peer-ip <ip_addr> | Enter the IP address of the secondary FortiMail unit. | 0.0.0.0 |
| failover <interface_str> {add \| bridge \| ignore \| set}<address_ipv4mask> | Use this option to configure whether and how to configure the IP addresses and netmasks of the primary FortiMail unit.<br>For example, a primary unit might be configured to receive email traffic through port1 and receive heartbeat and synchronization traffic through port5 and port6. In that case, you would configure the primary unit to set the IP addresses or add virtual IP addresses for port1 of the backup unit upon failover in order to mimic that of the primary unit.<br>This option applies only for FortiMail units operating in the active-passive HA mode, as a primary unit (The configuration of this command is synchronized to the backup unit for use when it assumes the role of the primary unit).<br>Enter the name of a network interface, such as `port6`, or enter `mgmt` to configure the management IP address (transparent mode only), then enter one of the following behaviors of the network interface when this FortiMail unit is acting as the primary unit:<br>`ignore`: Do not change the network interface configuration upon failover, and do not monitor. For details on service monitoring for network interfaces, see local-service {ports \| hd} <interval_int> <retries_int> on page 297. Primary and secondary heartbeat network interfaces must use this option.<br>`set`: Change the network interface to use the specified IP address and netmask upon failover.<br>`add`: Add the specified virtual IP address and netmask to the network interface upon failover. Normally, you will configure your network (MX records, firewall policies, routing and so on) so that clients and mail services use the virtual IP address. Both originating and reply traffic uses the virtual IP address. All replies to sessions with the virtual IP address include the virtual IP address as the source address. Originating traffic, however, will use the network interface's actual IP address as the source address. | |

| Variable | Description | Default |
|---|---|---|
| | `bridge`: Include the network interface in the Layer 2 bridge. While the effective operating mode is secondary, the interface is deactivated and cannot process traffic, preventing Layer 2 loops. Then, when the effective operating mode becomes primary, the interface is activated again and can process traffic. This option applies only if the FortiMail unit is operating in transparent mode, and for mail interfaces that are already members of the bridge. For information on configuring bridging network interfaces, see system interface on page 300.<br>Network interface(s) configured as the primary heartbeat and secondary heartbeat network interface are required to maintain their IP addresses for heartbeat and synchronization purposes, and cannot be configured with the type `set` or `bridge`.<br>After entering a network interface behavior, enter the IP address and netmask.<br>If you have entered `bridge` or `ignore` for the previous keyword, because those behaviors do not use IP addresses, you may enter `0.0.0.0 0.0.0.0`. | |
| hard-drives-check {enable \| disable} | Enable to test the responsiveness of the hard drives. | disable |
| hb-base-port <interface_int> | Enter the first of four total TCP port numbers that will be used for:<br>• the heartbeat signal<br>• synchronization control<br>• data synchronization<br>• configuration synchronization<br>**Note:** For active-passive groups, in addition or alternatively to configuring the heartbeat, you can configure service monitoring. | 20000 |
| hb-lost-threshold | Enter the total span of time, in seconds, for which the primary unit can be unresponsive before it triggers a failover and the backup unit assumes the role of the primary unit.<br>The heartbeat will continue to check for availability once per second. To prevent premature failover when the primary unit is simply experiencing very heavy load, configure a total threshold of three (3) seconds or more to allow the backup unit enough time to confirm unresponsiveness by sending additional heartbeat signals.<br>This option appears only for active-passive groups.<br>**Note:** If the failure detection time is too short, the backup unit may falsely detect a failure when during periods of high load.<br>**Caution:** If the failure detection time is too long the primary unit could fail and a delay in detecting the failure could mean that email is delayed or lost. Decrease the failure detection time if email is delayed or lost because of an HA failover. | 15 |

| Variable | Description | Default |
|---|---|---|
| heartbeat-1-interface <interface_int> | Enter the name of the network interface that will be used for the primary heartbeat, and that is connected directly or through a switch to the primary heartbeat interface of the other FortiMail unit(s) in the HA group. | Varies by model (the network interface with the highest number). |
| heartbeat-1-ip <local_ipv4mask> | Enter the IP address and netmask of the primary network interface, separated by a space.<br>Use this IP address as the value of the peer IP address when configuring heartbeat-1-peer <primary-peer_ipv4> on page 297 for the other FortiMail units in the HA group. | 10.0.0.1 255.255.255.0 |
| heartbeat-1-peer <primary-peer_ipv4> | Enter the IP address of the primary heartbeat network interface on the other FortiMail unit in the HA group.<br>For example, if the primary heartbeat network interface on the other FortiMail unit has an IP address of 10.0.0.1, enter 10.0.0.1. | 10.0.0.2 |
| heartbeat-2-interface <interface_str> | Enter the name of a network interface: Use this network interface as the secondary heartbeat network interface. It must be connected to the secondary heartbeat network interface on the other FortiMail unit in the HA group. Also configure `heartbeat-2-ip <secondary-local_ipv4mask>` on page 297. | Varies by model (the network interface with the highest number). |
| heartbeat-2-ip <secondary-local_ipv4mask> | Enter the IP address and netmask of the secondary network interface, separated by a space.<br>Use this IP address as the value of the peer IP address when configuring heartbeat-2-peer <secondary-peer_ipv4> on page 297 for the other FortiMail units in the HA group. | 0.0.0.0 0.0.0.0 |
| heartbeat-2-peer <secondary-peer_ipv4> | Enter the IP address of the secondary heartbeat network interface on the other FortiMail unit in the HA group.<br>For example, if the secondary heartbeat network interface on the other FortiMail unit has an IP address of 10.0.0.3, enter 10.0.0.3. | 0.0.0.0 |
| local-service {ports \| hd} <interval_int> <retries_int> | Enter a local service to monitor.<br>If you enter `ports`, continue entering:<br>`<interval_int>`: Enter the amount of time in seconds between each network interface check.<br>The valid range is between 1 and 60 seconds, or 0 to disable checking. The default value is 0.<br>`<retries_int>`: Enter the number of times a network interface must consecutively fail to respond in order to trigger a failover.<br>The valid range is 1 to a very high number. The default value is 0.<br>If you enter `hd`, continue entering: | PORTS 10 3<br>HD 10 3 |

| Variable | Description | Default |
|---|---|---|
| | `<interval_int>`: Enter the amount of time in seconds between each hard drive check.<br>The valid range is between 1 and 60 seconds, or 0 to disable checking. The default value is 0.<br>`<retries_int>`: Enter the number of times a hard drive must consecutively fail to respond in order to trigger a failover.<br>The valid range is 1 to a very high number. The default value is 0.<br>During local service monitoring, the primary unit in an active-passive HA group monitors its own network interfaces and hard drives. If either of these local services fails, the primary unit triggers a failover by switching its effective operating mode to “off," and no longer responding to the heartbeat of the backup unit. The backup unit then becomes the new primary unit.<br>If service monitoring detects a failure, the effective operating mode of the primary unit switches to OFF or FAILED (depending on the “On failure" setting) and, if configured, the FortiMail units send HA event alert email, record HA event log messages, and send HA event SNMP traps. A failover then occurs, and the effective operating mode of the backup unit switches to primary.<br>This command applies only if the FortiMail unit is operating in an active-passive HA group, as the primary unit. | |
| mail-data-sync {enable \| disable} | Enable to synchronize system quarantine, email archives, email users’ mailboxes (server mode only), preferences, and per-recipient quarantines.<br>Unless the HA cluster stores its mail data on a NAS server, you should configure the HA cluster to synchronize mail directories.<br>This option applies only for active-passive groups. | enable |
| mailqueue-data-sync {enable \| disable} | Enable to synchronize the mail queue of the FortiMail unit.<br>This option applies only for active-passive groups.<br>Caution: If the primary unit experiences a hardware failure and you cannot restart it, if this option is disabled, MTA spool directory data could be lost.<br>Note: Enabling this option is not recommended. Periodic synchronization can be processor and bandwidth-intensive. Additionally, because the content of the MTA spool directories is very dynamic, periodically synchronizing MTA spool directories between FortiMail units may not guarantee against loss of all email in those directories. Even if MTA spool directory synchronization is disabled, after a failover, a separate synchronization mechanism may successfully prevent loss of MTA spool data. | disable |
| mode {config-primary \| config-secondary \| primary \| off \| secondary} | Enter one of the following HA operating modes:<br>`config-primary`: Enable HA and operate as the primary unit in a config-only HA group.<br>`config-secondary`: Enable HA and operate as the backup unit in a config-only HA group.<br>`primary`: Enable HA and operate as the primary unit in an active-passive HA group.<br>`off`: Disable HA. Each FortiMail unit operates independently. | off |

| Variable | Description | Default |
|---|---|---|
| | `secondary`: Enable HA and operate as the backup unit in an active-passive HA group.<br>**Caution**: For config-only HA, if the FortiMail unit is operating in server mode, you must store mail data externally, on a NAS server. Failure to store mail data externally could result in mailboxes and other data scattered over multiple FortiMail units. For details on configuring NAS, see the *FortiMail Administration Guide*. | |
| network-intf-check {enable \| disable} | Enable to test the responsiveness of network interfaces.<br>Network interface monitoring tests all active network interfaces whose:<br>failover <interface_str> {add \| bridge \| ignore \| set}<address_ipv4mask> on page 295setting is **not** `ignore`<br>port-monitor {enable \| disable} on page 293 setting is `enable`. | enable |
| on-failure {off \| restore-role \| become-secondary} | Enter one of the following behaviors of the primary unit when it detects a failure.<br>`off`: Do not process email or join the HA group until you manually select the effective operating mode.<br>`restore-role`: On recovery, the failed primary unit's effective operating mode resumes its configured operating mode. This behavior may be useful if the cause of failure is temporary and rare, but may cause problems if the cause of failure is permanent or persistent.<br>`become-secondary`: On recovery, the failed primary unit's effective operating mode becomes secondary (backup), and it then synchronizes the content of its MTA spool directories with the current primary unit. The new primary unit can then deliver email that existed in the former primary unit's MTA spool at the time of the failover.<br>In most cases, you should enter `become-secondary`.<br>For details on the effects of this option on the effective operating mode, see the *FortiMail Administration Guide*. This option applies only if the FortiMail unit is operating in an active-passive HA group, as a primary unit. | |
| password <password_str> | Enter a password for the HA group. The password must be the same on the primary and backup FortiMail unit(s). The password must be a least 1 character. | change_me |
| remote-service {smtp \| pop \| imap \| http} <interface_ipv4> <port_int> <interval_int> <wait_int> <retries_int> | Enter a remote service to monitor. Then enter the subsequent values in order:<br>`<interface_ipv4>`: Enter the IP address to contact when testing the availability of the service. The default value is `0.0.0.0`.<br>`<port_int>`: Enter the TCP port number on which the remote FortiMail unit listens for connections of that service type. The default value is `0`.<br>For example, if you have configured the primary FortiMail unit to listen for SMTP connections on TCP port 25, you would enter `25`.<br>`<interval_int>`: Enter the interval in minutes between each remote service availability test.<br>The valid range is 1 to 60 minutes, or 0 to disable remote service monitoring. The default value is `0`. | |

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

## Related topics

system geoip-override on page 286
system ha on page 291

# 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 consist of those destined for the SMTP servers that are protected domains of the FortiMail unit. For example, if the FortiMail unit is configured to protect the SMTP server whose IP address is 10.1.1.1, the FortiMail

unit treats all SMTP connections destined for 10.1.1.1 as incoming. For information about configuring protected domains, see config domain-setting on page 105.

Outgoing connections consist of those destined for SMTP servers that the FortiMail unit has not been configured to protect. For example, if the FortiMail unit is **not** configured to protect the SMTP server whose IP address is 192.168.1.1, all SMTP connections destined for 192.168.1.1 will be treated as outgoing, regardless of their origin.

## Syntax

```
config system interface
  edit <physical_interface_str> on page 301, <logical_interface_str> on page 301,
       or loopback on page 301
    set allowaccess {ping http https snmp ssh telnet} on page 302
    set bridge-member {enable | disable}
    set ip <ipv4mask> on page 302
    set ip6 <ipv6mask> on page 302
    set mac-addr <xx.xx.xx.xx.xx.xx> on page 303
    set mailaccess {imap | imaps | pop3 | pop3s | smtp | smtps} on page 303
    set mode {static | dhcp} on page 303
    set mtu <mtu_int> on page 303
    set proxy-smtp-in-mode {pass-through | drop | proxy} on page 303
    set proxy-smtp-local status {enable | disable} on page 303
    set proxy-smtp-out-mode {pass-through | drop | proxy} on page 304
    set speed {auto | 10full | 10half | 100full | 100half | 1000full} on page
        305
    set status {down | up} on page 305
    set type {vlan | redundant} on page 304
    set vlanid <int> on page 305
    set webaccess on page 305
    set redundant-link-monitor {mii-link | arp-link} on page 305
    set redundant-arp-ip <ip_addr> on page 304
    set redundant-member <member_interface_str> on page 305
end
```

| Variable | Description | Default |
|---|---|---|
| <physical_ interface_str> | Enter the name of the physical network interface, such as port1. | |
| <logical_interface_ str> | 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.<br>The FortiMail's loopback IP address does not depend on one specific external port, and is therefore possible to access through several physical or VLAN interfaces. In the current release, you can only add one loopback interface on the FortiMail unit.<br>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. | |

| Variable | Description | Default |
|---|---|---|
| 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:<br>• `ping`: Allow ICMP ping responses from this network interface.<br>• `http`: Allow HTTP access to the web-based manager, webmail, and per-recipient quarantines.<br>**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.<br>• `https`: Allow secure HTTP (HTTPS) access to the web-based manager, webmail, and per-recipient quarantines.<br>• `snmp`: Allow SNMP v2 access. For more information, see system snmp community on page 316, system snmp sysinfo on page 317, and system snmp threshold on page 318.<br>• `ssh`: Allow SSH access to the CLI.<br>• `telnet`: Allow Telnet access to the CLI.<br>To control SMTP access, configure access control rules and session profiles. For details, see ms365 profile antivirus on page 151 and profile session on page 235.<br>**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. | Varies by network interface. |
| bridge-member {enable \| disable} | **Note**: This command is only available when the FortiMail unit is operating in Transparent mode, and only for non-management ports.<br>Enable to bridge the port to the management IP. See Editing network interfaces for information on bridged networks in transparent mode.<br>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.<br>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. | enable |
| ip <ipv4mask> | Enter the IP address and netmask of the network interface.<br>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. | |

| Variable | Description | Default |
|---|---|---|
| | 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> | Override the factory set MAC address of this interface by specifying a new MAC address. Use the form xx:xx:xx:xx:xx:xx. | Factory set |
| mailaccess {imap \| imaps \| pop3 \| pop3s \| smtp \| smtps} | Allow mail access with the interface. | |
| mode {static \| dhcp} | Enter the interface mode.<br>DHCP mode applies only if the FortiMail unit is operating in gateway mode or server mode. | static |
| mtu <mtu_int> | Enter the maximum packet or Ethernet frame size in bytes.<br>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.<br>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:<br>• `pass-through`: Permit but do not proxy or relay. Because traffic is not proxied or relayed, no policies will be applied.<br>• `drop`: Drop the connection.<br>• `proxy`: Proxy or relay the connection. Once intercepted, policies determine any further scanning or logging actions. For more information, see config policy delivery-control on page 159, policy recipient on page 163, and config policy recipient on page 115.<br>**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*.<br>This option is only available in transparent mode. | proxy |
| proxy-smtp-local status {enable \| disable} | Enable to allow connections destined for the FortiMail unit itself.<br>This option is only available in transparent mode. | disable |

| Variable | Description | Default |
|---|---|---|
| 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:<br>• `pass-through`: Permit but do not proxy or relay. Because traffic is not proxied or relayed, no policies will be applied.<br>• `drop`: Drop connections.<br>• `proxy`: Proxy or relay connections. Once intercepted, policies determine any further scanning or logging actions. For more information, see config policy delivery-control on page 159.<br>**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*.<br>This option is only available in transparent mode. | pass-through |
| redundant-arp-ip <ip_addr> | Enter the redundant interface ARP monitoring IP target.<br>This option is only available when you choose the `arp-link` monitoring parameter. See redundant-link-monitor {mii-link \| arp-link} on page 305. | |
| type {vlan \| redundant} | `vlan`: A Virtual LAN (VLAN) subinterface, also called a VLAN, is a virtual interface on a physical interface. The subinterface allows routing of VLAN tagged packets using that physical interface, but it is separate from any other traffic on the physical interface.<br>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.<br>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.<br>Also configure redundant-link-monitor {mii-link \| arp-link} on page 305 and redundant-member <member_interface_str> on page 305.<br>`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.<br>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.<br>Also configure vlanid <int> on page 305. | |

| Variable | Description | Default |
|---|---|---|
| redundant-link-monitor {mii-link \| arp-link} | Configure the parameters to monitor the connections of the redundant interfaces. This option is only available when you choose the `redundant` interface type. `mii-link`: Media Independent Interface is an abstract layer between the operating system and the NIC which detects whether the failover link is running.<br>`arp-link`: Address Resolution Protocol periodically checks whether the remote interface is reachable. Also configure redundant-arp-ip <ip_addr> on page 304. | mii-link |
| redundant-member <member_interface_str> | Enter the redundant member for the failover configuration.<br>This option is only available when you choose the `redundant` interface type. | |
| vlanid <int> | Enter the Vlan ID for logically separating devices on a network into smaller broadcast domains.<br>This option is only available when you choose the `vlan` interface type. | |
| webaccess | Allow web access with the interface. | |
| speed {auto \| 10full \| 10half \| 100full \| 100half \| 1000full} | Enter the speed of the network interface.<br>**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 on page 253

system admin on page 256

# system link-monitor

Use this command to propagate status of a sort to other ports.

## Syntax

```
config system link-monitor
   set link-monitor-delay on page 306
   set link-monitor-interval on page 306
   set link-monitor-status {enable | disable} on page 306
end
```

| Variable | Description | Default |
|---|---|---|
| link-monitor-delay | Enter in seconds the amount of time to delay after link state changes. | |
| 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 the system-wide mail settings.

## Syntax

```
config system mailserver
   config mail-queue
      edit {default | incoming | outgoing} on page 307
         set queue-dsn-timeout <timeout_int> on page 309
         set queue-retry <interval_int> on page 309
         set queue-timeout <timeout_int> on page 309
         set queue-warning <first-dsn_int> on page 310
      end
   set deadmail-expiry <time_int> on page 307
   set default-auth-domain <domain_name> on page 307
   set defer-delivery-starttime <time_str> on page 307
   set defer-delivery-stoptime <time_str> on page 307
   set delivery-esmtp {no | yes} on page 307
   set delivery-failure-conditions {dns-failure | mta-failure-permanant | mta-
        failure-temporary | network-failure-connection | network-failure-other}
        on page 307
   set delivery-failure-handling-option {normal | relay-to-host} on page 308
   set delivery-failure-host <host_name> on page 308
   set delivery-failure-min-age <minute_int> on page 308
   set dsn-ehlo-option {host-name | domain-name | other-name} on page 308
   set dsn-ehlo-other-name <name_str> on page 308
   set dsn-sender-address <email_str> on page 308
   set dsn-sender-displayname <name_str> on page 308
   set dsn-status {enable | disable} on page 308
   set imap-service {enable | disable} on page 308
   set system mailserver
   set ldap-domaincheck {enable | disable} on page 308
   set ldap-domaincheck-auto-associate {enable | disable} on page 309
   set ldap-domaincheck-internal-domain <domain_str> on page 309
   set ldap-domaincheck-profile <profile_str> on page 309
   set local-domain-name <local-domain_str> on page 309
   set pop3-port <port_int> on page 309
   set pop3-service {enable | disable} on page 309
   set queue-dsn-timeout <timeout_int> on page 309
   set queue-retry <interval_int> on page 309
   set queue-timeout <timeout_int> on page 309
   set queue-warning <first-dsn_int> on page 310
```

```
    set relay-server-name <relay_name> on page 310
    set relay-server-status {enable |disable} on page 310
    set show-accept-cert-ca {enable | disable} on page 310
    set smtp-auth {enable | disable} on page 310
    set smtp-auth-over-tls {enable | disable} on page 310
    set smtp-auth-smtps {enable | disable} on page 310
    set smtp-delivery-addr-pref {ipv4-ipv6 | ipv6-ipv4 | ipv4 | ipv6} on page 310
    set smtp-delivery-session-preference {domain | host}
    set smtp-max-connections <connection_int> on page 311
    set smtp-max-hop-count <number> on page 311
    set smtp-msa {enable | disable} on page 311
    set smtp-msa-port <port_int> on page 311
    set smtp-mtasts-status {check-all-domain | check-external-domain | disable}
    set smtp-port <port_int> on page 311
    set smtp-service {enable | disable} on page 311
    set smtps-port <port_int on page 311
    set smtps-tls-status {enable | disable} on page 311
    set timeout-connect <seconds_int> on page 311
    set timeout-greeting <seconds_int> on page 311
end
```

| Variable | Description | Default |
|---|---|---|
| deadmail-expiry <time_int> | Enter the number of days to keep permanently undeliverable email in the dead mail folder. Dead mail has both incorrect recipient and sender email addresses, and can neither be delivered nor the sender notified.<br>The valid range is from 1 to 365 days. | 1 |
| default-auth-domain <domain_name> | Enter the domain to use for default authentication. | |
| {default \| incoming \| outgoing} | Select the queue 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:<br>`yes`: Disable the FortiMail unit from delivering email using ESMTP, and use standard SMTP instead.<br>`no`: Enable the FortiMail unit to deliver email using ESMTP if the SMTP server to which it is connecting supports the protocol. | no |
| delivery-failure-conditions {dns-failure \| mta-failure-permanant \| mta-failure-temporary \| network-failure-connection \| network-failure-other} | Specify the type of failed network connections the backup relay should take over and retry. | |

| Variable | Description | Default |
|---|---|---|
| delivery-failure-handling-option {normal \| relay-to-host} | When email delivery fails, you can choose to use the mail queue settings to handle the temporary or permanent failures. You can also try another relay that you know might work.<br>`normal`: Enter this option if you want to queue the email and use the mail queue settings.<br>`relay-to-host`: Enter another relay (backup relay) that you want to use for failed deliveries. | normal |
| delivery-failure-host <host_name> | Enter a host to relay email when access to original mail host fails. | |
| delivery-failure-min-age <minute_int> | Enter the time in minutes the undelivered email should wait in the normal queue before trying the backup relay. | 30 |
| dsn-ehlo-option {host-name \| domain-name \| other-name} | Specify the DSN EHLO/HELO argument to use:<br>• host-name: use the host name of the FortiMail unit.<br>• domain-name: use the local domain name of the FortiMail unit.<br>• other-name: use the customized name. Then use the below command to specify the name. | host-name |
| dsn-ehlo-other-name <name_str> | If you specify to use other-name in the above command, use this command to enter the customized name. | |
| dsn-sender-address <email_str> | Enter the sender email address in delivery status notification (DSN) email messages sent by the FortiMail unit to notify email users of delivery failure.<br>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.<br>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.<br>You can exempt IP pool usage for internal-to-internal email using the `exclude-internal-to-internal` option.<br>Note that 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> on page 309` and `ldap-domaincheck-auto-associate {enable \| disable} on page 309`. | disable |

| Variable | Description | Default |
|---|---|---|
| | 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}` on page 309. | |
| ldap-domaincheck-auto-associate {enable \| disable} | If `ldap-domaincheck` is `enable`, select whether to enable or disable automatic creation of domain associations.<br>`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>` on page 309.<br>`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 163. | disable |
| ldap-domaincheck-internal-domain <domain_str> | If `ldap-domaincheck` is `enable`, and `ldap-domaincheck-auto-associate` is `enable`, enter name of the protected domain with which successfully verified domains will become associated. | |
| ldap-domaincheck-profile <profile_str> | If `ldap-domaincheck` is `enable`, enter the name of the LDAP profile to use when verifying unknown domains. | |
| local-domain-name <local-domain_str> | Enter the name of the domain to which the FortiMail unit belongs, such as `example.com`.<br>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.<br>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 <timeout_int> | Enter the maximum number of days a delivery status notification (DSN) message can remain in the mail queues. If the maximum time is set to zero (0) days, the FortiMail unit attempts to deliver the DSN only once.<br>After the maximum time has been reached, the DSN email is moved to the dead mail folder.<br>The valid range is from zero to ten days. | 5 |
| queue-retry <interval_int> | Enter the number of minutes between delivery retries for email messages in the deferred and spam mail queues.<br>The valid range is from 10 to 120 minutes. | 27 |
| queue-timeout <timeout_int> | Enter the maximum number of hours that deferred email messages can remain in the deferred or spam mail queue, during which the FortiMail unit periodically retries to send the message. | 120 |

| Variable | Description | Default |
|---|---|---|
| | After the maximum time has been reached, the FortiMail unit will send a final delivery status notification (DSN) email message to notify the sender that the email message was undeliverable.<br>The valid range is from 1 to 240 hours. | |
| queue-warning <first-dsn_int> | Enter the number of hours after an initial failure to deliver an email message before the FortiMail unit sends the first delivery status notification (DSN) email message to notify the sender that the email message has been deferred.<br>After sending this initial DSN, the FortiMail unit will continue to retry sending the email until reaching the limit configured in `timeout`.<br>The valid range is from 1 to 24 hours. | 4 |
| relay-server-name <relay_name> | Specify the relay server to deliver outgoing email. | |
| 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.<br>Use this command to specify the IPv4/IPv6 delivery preferences:<br>• `ipv4-ipv6`: Try to deliver to the IPv4 address frist. If the IPv4 address is not accessible, try the IPv6 address. Because most MTAs support IPv4, this is the default setting.<br>• `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.<br>• `ipv4`: Try IPv4 only. This setting is not recommended.<br>• `ipv6`: Try IPv6 only. This setting is not recommended. | ipv4-ipv6 |
| smtp-delivery-session-preference {domain \| host} | Google business email service does not accept multiple destination domains per SMTP transaction, resulting in repeated delivery attempts and delayed email. To work around this Google limitation, this command is added in 5.4.6 and 6.0.1 releases.<br>Before 5.4.6 and 6.0. releases, the default setting is host. Multiple recipient domains that resolve to the same MTA are sent to the server in the same session. | domain |

| Variable | Description | Default |
|---|---|---|
| | After 5.4.6 and 6.0.1 release, the default setting is changed to domain. Multiple recipient domains that resolve to the same MTA are sent to the server in separate sessions. | |
| smtp-max-connections <connection_int> | Enter the maximum number of concurrent SMTP connections that FortiMail can accept from the STMP clients. | Platform dependent |
| smtp-max-hop-count <number> | 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.<br>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:<br>• `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.<br>• `check-external-domain`: FortiMail MTA-STS checking only when delivering outgoing emails to external domains.<br>• `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 |
| 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.<br>When disabled, SMTP connections with the FortiMail unit's built-in MTA must occur as clear text, unencrypted. | disable |
| timeout-connect <seconds_int> | Enter the maximum amount of time to wait, after the FortiMail unit initiates it, for the receiving SMTP server to establish the network connection.<br>The valid range is 10 to 120.<br>**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.<br>The valid range is 10 to 360. | 30 |

| Variable | Description | Default |
|---|---|---|
| | **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. | |

## Related topics

system route on page 314

# 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} on page 312
   set apply-to {admin-user | ibe-user | local-mail-user} on page 312
   set minimum-length <minimum_int> on page 312
   set must-contain {upper-case-letter | lower-case-letter | number | non-
        alphanumeric} on page 313
   set allow-admin-empty-password {enable | disable} on page 313
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:<br>• `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.<br>• `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.<br>• `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 |

| Variable | Description | Default |
|---|---|---|
| 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.<br>`upper-case-letter` — A, B, C, ... Z<br>`lower-case-letter` — a, b, c, ... z<br>`number` — 0, 1, 2, 3, 4, 5, 6, 7 8, 9<br>`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 on page 305

# 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> on page 314
      set destination <destination_ipv4mask> on page 314
      set gateway <gateway_ipv4> on page 314
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> on page 314
      set destination <destination_ipv4mask> on page 314
      set gateway <gateway_ipv4> on page 314
      set interface <interface_name> on page 314
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.<br>To indicate all traffic regardless of IP address and netmask, enter `0.0.0.0 0.0.0.0`. | 0.0.0.0 0.0.0.0 |
| gateway <gateway_ipv4> | Enter the IP address of the gateway router. | 0.0.0.0 |
| interface <interface_name> | Enter the interface name that you want to add the static route to. | |

## Related topics

system link-monitor on page 305

# system saml

Use this command to enable and configure SAML SSO.

## Syntax

```
config system saml
   set status {enable | disable} on page 314
   set idp-metadata-url <url> on page 314
end
```

| Variable | Description | Default |
|---|---|---|
| status {enable \| disable} | Enable or disable the feature. | disable |
| idp-metadata-url <url> | Specify the URL to retrieve the IDP metadata. | |

# system scheduled-backup

Use this command to configure system backup.

## Syntax

```
config system scheduled-backup
   set destination...
end
```

| Variable | Description | Default |
|---|---|---|
| destination... | Configure the destination server and schedule. | |

# system security crypto

Use this command to modify protocol specific crypto configuration.

## Syntax

```
config system security crypto
   edit http
      set custom-ciphers <ciphers> on page 315
      set dh-params {1024 | 2048 | 3072 | 4096} on page 315
      set ssl-versions {tls1_0 | tls1_1 | tls1_2 | tls1_3} on page 316
      set status {enable | disable} on page 316
      set strong-crypto {enable | disable} on page 316
   edit mail
      set custom-ciphers <ciphers> on page 315
      set dh-params {1024 | 2048 | 3072 | 4096} on page 315
      set ssl-versions {tls1_0 | tls1_1 | tls1_2 | tls1_3} on page 316
      set status {enable | disable} on page 316
      set strong-crypto {enable | disable} on page 316
end
```

| Variable | Description | Default |
|---|---|---|
| custom-ciphers <ciphers> | Add ciphers by typing +cipher_names separated by spaces, such as +RC4-SHA +CAMELLIA256-SHA. Delete ciphers by typing -cipher_names separated by spaces, such as -RC4-SHA -CAMELLIA256-SHA.<br>Type ? to see all the supported regular and strong ciphers. The available ciphers for addition are listed under *Available ciphers*; the *Selected ciphers* list the ones that have already been added. You can remove ciphers from the *Selected ciphers* list. | |
| dh-params {1024 \| 2048 \| 3072 \| 4096} | Enter the minimum size in bits of the Diffie-Hellman prime. | 1024 |

| Variable | Description | Default |
|---|---|---|
| ssl-versions {tls1_0 \| tls1_1 \| tls1_2 \| tls1_3} | Enter the SSL protocol version enabled. | tls1_1, tls1_2, tls1_3 |
| status {enable \| disable} | Enable the protocol specific crypto. | disable |
| strong-crypto {enable \| disable} | Use strong ciphers and digests. | enable |

# 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 on page 316
           set sender-ip-mask on page 316
        end
     set access-group {cli mail web} on page 316
     set block-period <minutes> on page 316
     set status (disable | enable | monitor-only) on page 316
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} on page 318.

## 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 on page 317
system snmp threshold on page 318

# 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> on page 317
   set description <description_str> on page 318
   set port-https <port_int> on page 290
   set location <location_str> on page 318
   set status {enable | disable} on page 318
end
```

| Variable | Description | Default |
|---|---|---|
| contact <contact_str> | Enter the contact information for the administrator of this FortiMail unit, such as 'admin@example.com'. | |

| Variable | Description | Default |
|---|---|---|
| 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 on page 316
system snmp threshold on page 318

# 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> on page
        318
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:<br>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.<br>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.<br>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. | cpu: 80 3 600 30<br>mem: 80 3 600 30<br>logdisk: 90 1 7200 3600<br>maildisk: 90 1 7200 3600 |

| Variable | Description | Default |
|---|---|---|
| | `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. | virus: 10 600<br><br>spam: 60 600 |

## Related topics

system snmp community on page 316
system snmp sysinfo on page 317

# 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> on page 319
      set query-status {enable | disable} on page 320
      set query-port <port_number> on page 320
      set security-level {authnopriv | authpriv | noauthnopriv} on page 320
      set auth-proto {sha1 | md5} on page 320
      set aut-pwd <password> on page 320
      set status {enable | disable} on page 320
      set trap-status {enable | disable} on page 320
      set trapevent {cpu | deferred-queue | ha | ip-change | logdisk | mem | raid
          | remote-storage | spam | system | virus} on page 320
      set trapport-local <port_number> on page 321
      set trapport-remote <port_number> on page 321
   config host
      edit <host_no> on page 321
         set ip <class_ip> on page 321
   end
end
```

| Variable | Description | Default |
|---|---|---|
| <user_name> | Enter a name to identify the SNMP user on FortiMail. | |

| Variable | Description | Default |
|---|---|---|
| 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.<br>• `noauthnotpriv` (no authentication, no privacy): This option is similar to SNMP v1 and v2.<br>• `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).<br>• `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. | |
| 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:<br>• `cpu`: CPU usage threshold<br>• `deferred-queue`: Deferred queue threshold<br>• `ha`: High availability (HA) event<br>• `ip-change`: Interface IP address change<br>• `logdisk`: Log disk space low threshold<br>• `maildisk`: Mail disk space low threshold<br>• `mem`: Memory low threshold<br>• `raid`: RAID event<br>• `remote-storage`: NAS storage related events<br>• `spam`: Spam threshold<br>• `system`: System events, such as a change in the state of hardware, power failure and so on.<br>• `virus`: Virus threshold<br>**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.<br>To set SNMP trap thresholds for the event types that use them, see system snmp threshold on page 318. | cpu<br>deferred-queue<br>ha<br>logdisk<br>maildisk<br>mem<br>raid<br>remote-storage<br>system |

| Variable | Description | Default |
|---|---|---|
| | Events apply only when traps are enabled in . | |
| 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 on page 316
system snmp sysinfo on page 317

# 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 322.

## Syntax

```
config system time manual
   set daylight-saving-time {disable | enable} on page 321
   set zone <zone_int> on page 321
end
```

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

## Related topics

system time ntp on page 322

# 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 321.

## Syntax

```
config system time ntp
   set ntpserver {<address_ipv4> | <fqdn_str>} on page 322
   set ntpsync {enable | disable} on page 322
   set syncinterval <interval_int> on page 322
end
```

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

## Related topics

system time manual on page 321

# 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 on page 323
    set id on page 323
    set local-ip on page 323
    set password on page 323
    set remote-ip on page 323
    set status on page 323
  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 finer rate limit controls for REST API and other web services, allowing for greater control of server responses to the web service requests.

Value ranges for certain commands vary and are dependent on FortiMail model.

## Syntax

```
config system web-service
  config exempt-list
    edit <id>
      set <ip&netmask_str>
    next
  end
  set https-redirect-host <string>
  set https-redirect-status {enable | disable}
  set max-active-session-admin <integer>
  set max-active-session-restful <integer>
  set max-concurrent-request-admin <integer>
  set max-concurrent-request-all <integer>
  set max-concurrent-request-ms365 <integer>
  set max-concurrent-request-per-ip <integer
  set max-concurrent-request-restful <integer>
  set max-concurrent-request-webmail <integer>
  set max-request-rate-admin <integer>
  set max-request-rate-ms365 <integer>
```

```
    set max-request-rate-restful <integer>
    set max-request-rate-webmail <integer>
    set repeat-offender-status {enable | disable} on page 325
    set repeat-offender-count <integer> on page 325
    set repeat-offender-period <integer> on page 325
    set rest-api-status {enable | disable}
end
```

| Variable | Description | Default |
|---|---|---|
| exempt-list | Configure exempt lists of those IP addresses you wish to exempt from rate limits. | |
| https-redirect-host <string> | Enter the host name for HTTPS redirection | |
| https-redirect-status {enable \| disable} | Enable to redirect HTTP to HTTPS. | enable |
| max-active-session-admin <integer> | Enter the maximum number of active administrator sessions. | 200 |
| max-active-session-restful <integer> | Enter the maximum number of active RESTful sessions. | 10 |
| max-concurrent-request-admin <integer> | Enter the maximum number of concurrent admin portal requests. | 50 |
| max-concurrent-request-all <integer> | Enter the maximum number of concurrent HTTP requests from all clients. | 0 |
| max-concurrent-request-ms365 <integer> | Enter the maximum number of concurrent Microsoft 365 requests permitted. | 100 |
| max-concurrent-request-per-ip <integer | Enter the maximum number of concurrent HTTP requests for a single IP address. | 0 |
| max-concurrent-request-restful <integer> | Enter the maximum number of concurrent RESTful requests. | 20 |
| max-concurrent-request-webmail <integer> | Enter the maximum number of concurrent webmail portal requests. | 200 |
| max-request-rate-admin <integer> | Enter the maximum request rate (per second) for administrators. | 0 |
| max-request-rate-ms365 <integer> | Enter the maximum request rate (per second) for Microsoft 365. | 100 |
| max-request-rate-restful <integer> | Enter the maximum request rate (per second) for the REST API. | 50 |
| max-request-rate-webmail <integer> | Enter the maximum request rate (per second) for webmail. | 0 |

| Variable | Description | Default |
|---|---|---|
| repeat-offender-status {enable \| disable} | Enable to block the IP addresses that keep sending bad HTTP requests to FortiMail and causing FortiMail to return HTTP 404 or 405 errors. | enable |
| repeat-offender-count <integer> | Specify the number limit of bad requests within a specified period of time that will trigger offender IP blocking. The valid range is 1 to 50, and the default value is 5. | 5 |
| repeat-offender-period <integer> | Specify the period of time (in minutes) to count the bad requests. The valid range is 1 to 120, and the default value is 3. | 3 |
| rest-api-status {enable \| disable} | Enable or disable REST API access. | disable |

# system webfilter local-category

Use this command to view custom FortiGuard URL local filter categories for URL override rating profiles.

Use the `get` sub-command to list the entries' `group` and `id`, which are otherwise only configurable within the GUI.

## Syntax

```
config system webfilter local-category
   edit <name>
      set description <description>
   next
end
```

| Variable | Description | Default |
|---|---|---|
| description <description> | Optional description of the local category. | |

# system webfilter local-rating

Use these commands to configure URL rating patterns (as either wildcard or regular expressions) and override to defined URL categories. URL override rating lists can be used as web filter categories.

## Syntax

```
config system webfilter local-rating
   edit <id>
      set category <datasource>
      set description <description>
      set pattern-type {wildcard | regex}
      set status {enable | disable}
      set url-pattern <string>
   next
```

```
end
```

| Variable | Description | Default |
|---|---|---|
| category <datasource> | Enter a predefined category that the local rating overrides to.<br>Enter `set category ?` to view the list of categories available. | local |
| description <description> | Optional description of the local rating. | |
| pattern-type {wildcard \| regex} | Set the URL pattern type to either wildcard or regular expression. | wildcard |
| status {enable \| disable} | Enable or disable the local rating. | enable |
| url-pattern <string> | Enter the URL pattern, as either wildcard or regular expression. | |

# 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> on page 326
      set name <language-name_str> on page 326
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 on page 120

# 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 216.

## Syntax

```
config user alias
   edit name <email-alias_str> on page 327
      set member <recipient_str> on page 327
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 on page 328
user pki on page 330

# 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:<br>`MAIL FROM:`<br>`RCPT TO:`<br>`From:`<br>`To:`<br>`Return-Path:`<br>`Cc:`<br>`Reply-To:`<br>`Return-Receipt-To:`<br>`Resent-From:` | External email address |

| Order of evaluation | Match condition | If yes... | Rewrite to... |
|---|---|---|---|
| | | `Resent-Sender:`<br>`Delivery-Receipt-To:`<br>`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. For details, see profile ldap on page 216.

## Syntax

```
config user map
   edit encryption-profile <profile_str> on page 158
      set external-name <pattern_str> on page 330
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.<br>This email address will be rewritten into `external-name <pattern_str> on page 330` according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings: on page 328.<br>**Note**: If you enter a pattern with a wild card (`*` or `?`):<br>You must enter a pattern using the same wild card in `external-name <pattern_str> on page 330`. 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.<br>`external-name <pattern_str> on page 330` 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. | |

| Variable | Description | Default |
|---|---|---|
| external-name <pattern_str> | Enter either an email address, such as `user2@example.com`, or an email address pattern, such as `*@example.net`, that exists in a protected domain.<br>This email address will be rewritten into `encryption-profile <profile_str> on page 158` according to the match conditions and effects described in Match evaluation and rewrite behavior for email address mappings: on page 328.<br>**Note**: If you enter a pattern with a wild card (`*` or `?`):<br>You must enter a pattern using the same wild card in `encryption-profile <profile_str> on page 158`. 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.<br>`encryption-profile <profile_str> on page 158` 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 on page 322

# 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} on page 116` in config policy recipient on page 115 for email users, and `pki-certificate-req {yes | no} on page 289` in system geoip-override on page 286 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 more information, see "CA certificate".
- 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 256.
- 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} on page 290` in the command system geoip-override on page 286.

## Syntax

```
config user pki
   edit name <name_str> on page 331
      set ca <certificate_str> on page 331
      set domain <protected-domain_str> on page 332
      set ldap-field {cn | subjectalternative} on page 332
      set ldap-profile <profile_str> on page 332
      set ldap-query {enable | disable} on page 332
      set ocsp-ca <remote-certificate_str> on page 332
      set ocsp-check {enable | disable} on page 332
      set ocsp-unavailable-action {revoke | ignore} on page 332
      set ocsp-url <url_str> on page 332
      set subject <subject_str> on page 332
end
```

| Variable | Description | Default |
|---|---|---|
| name <name_str> | Enter the name of the PKI user. | |
| ca <certificate_ str> | Enter the name of the CA certificate used when verifying the CA's signature of the client certificate. For information on uploading a CA certificate, see the *FortiMail Administration Guide*.For more information, see "CA certificate". | |

| Variable | Description | Default |
|---|---|---|
| | If you configure an empty string for this variable, you must configure `subject <subject_str> on page 332`. | |
| domain <protected-domain_str> | Enter the name of the protected domain to which the PKI user is assigned, or enter `system` if the PKI user is a FortiMail administrator and belongs to all domains configured on the FortiMail unit. For more information on protected domains, see dlp scan-rules on page 100. | |
| 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).<br>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.<br>This variable is used only if `ldap-query` is `enable`. | subject |
| ldap-profile <profile_str> | Enter the LDAP profile to use when querying the LDAP server for the PKI user's existence. For more information on LDAP profiles, see profile ldap on page 216.<br>This variable is used only if `ldap-query` is `enable`. | |
| ldap-query {enable \| disable} | Enable to query an LDAP directory, such as Microsoft Active Directory, to determine the existence of the PKI user who is attempting to authenticate. Also configure `ldap-profile <profile_str> on page 332` and `ldap-field {cn \| subjectalternative} on page 332`. | 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".<br>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> on page 332`, `[ocsp-ca <remote-certificate_str> on page 332`, and `ocsp-unavailable-action {revoke \| ignore} on page 332`. | 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.<br>This option applies only if `oscp-check` is `enable`. | ignore |
| ocsp-url <url_str> | Enter the URL of the OCSP server.<br>This option applies only if `oscp-check` is `enable`. | |
| subject <subject_str> | Enter the value which must match the "subject" field of the client certificate. If empty, matching values are not considered when validating the client certificate presented by the PKI user's web browser.<br>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.<br>To disable Subject verification, enter an empty string surrounded by single quotes ( `''` ). | |

| Variable | Description | Default |
| --- | --- | --- |
| | If you configure an empty string for this variable, you must configure `ca <certificate_str>` on page 331. | |

## Related topics

system wccp settings on page 322
user map on page 328

# 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 the local machine.

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} on
    page 335 {ftp | local | scp | tftp} on page 335
```

| Variable | Description | Default |
|---|---|---|
| {config \| full-config \| ibe-data \| mail-queue \| user-config} | Type either:<br>• `config`: Back up configuration changes only. The default settings will not be backed up.<br>• `full-config`: Back up the entire configuration file (no default settings either), including the IBE data and user config.<br>• `ibe-data`: Back up the IBE data.<br>• `mail-queue`: Back up the mail queues.<br>• `user-config`: Back up the user-specific configurations, such as user preferences, personal block/safelists, and secondary addresses. Before backing up, you should update the user configuration file. To update the configurations, see user-config on page 375. | |
| {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...
```

## Optionally encrypt backup content

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.

### Example

```
execute backup config tftp config1.cfg 1.1.1.1
<Enter>|<passwd> Optional password to protect the backup content.
```

## Related topics

restore config on page 365
user-config on page 375

# backup-restore

Use this command to back up or restore email users' mailboxes. Before using this command, you must specify the backup destination or the restore location first. For details, see system backup-restore-mail on page 261.

## Syntax

```
execute backup-restore all-restore on page 336
execute backup-restore check-device on page 336
execute backup-restore format-device on page 336
execute backup-restore old-restore <full_int> <increments_int> domain <domain_str>
     user <user_str> on page 336
execute backup-restore restore {domain <domain> user <user> | host <host>} on page
     336
execute backup-restore start on page 337
execute backup-restore stop on page 337
```

| Variable | Description | Default |
|---|---|---|
| all-restore | Use this command to restore mail data without deleting previous full restore while restoring incremental backup. | |
| check-device | Performs file system check on the backup device. | |
| format-device | Format the backup device as a preparation step before backup. | |
| old-restore <full_int> <increments_int> domain <domain_str> user <user_str> | <full_int> is the full backup version you specify when you configure the backup settings.<br><increments_int> is the number of incremental backups to make between each full backup.<br><domain_str>: optionally specify which domain's mailbox will be restored.<br><user_str>: optionally specify which user's mailbox will be restored.<br>For details, see system backup-restore-mail on page 261. | |
| restore {domain <domain> user <user> \| host <host>} | Restores mailboxes, or optionally, for the specified domain or user.<br>If you want to restore mailboxes from backups identified by another FQDN, such as a previous FQDN or the FQDN of another FortiMail unit, specify the <host>, which is the FQDN.<br>Usually, you should enter an FQDN of this FortiMail unit, but you may enter only the host name if the local domain name is not configured, or enter the FQDN of another FortiMail unit if you want to import that FortiMail unit's mailbox backup. | |

| Variable | Description | Default |
|---|---|---|
| | For example, you may be upgrading to a FortiMail-2000 from a FortiMail-400. Previously, you have used a USB disk to store a backup of the mailboxes of the FortiMail-400, whose fully qualified domain name (FQDN) was fortimail.example.com. You have then configured the FortiMail-2000 to also use the USB disk as its backup media. You could then import the FortiMail-400's mailbox backup to the FortiMail-2000 by entering `fortimail.example.com` in this field on the FortiMail-2000's web UI. | |
| start | Initiate an immediate backup. Note that all data on the backup device will be erased. | |
| stop | Stops any currently running backups. | |

## Related topics

restore config on page 365
backup on page 334

# blocklist

Use this command to configure blocklist operations.

## Syntax

```
execute blocklist add
execute blocklist backup
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):<br>`execute blocklist add [domain \| user] <domain-name \| user-name> <list-content>`<br>`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):<br>`execute blocklist backup [domain \| user] <domain-name \| user-name> <tftp-server-ip> <file-name>`<br>`execute blocklist backup [system] <tftp-server-ip> <file-name>` | |
| purge | Purge a domain or user level blocklist, or system level blocklist, as shown below (respectively):<br>`execute blocklist purge [domain \| user] <domain-name-list \| user-name-list>`<br>`execute blocklist purge [system]` | |

| Variable | Description | Default |
|---|---|---|
| remove | Remove a domain or user level blocklist, or system level blocklist, as shown below (respectively):<br>`execute blocklist remove [domain \| user] <domain-name \| user-name> <list-content>`<br>`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):<br>`execute blocklist restore [domain \| user] <domain-name \| user-name> <tftp-server-ip> <file-name>`<br>`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> on page 338
execute certificate ca export tftp <cert_name> <file_name> <tftp_ip> on page 338
execute certificate config verify on page 339
execute certificate crl import tftp <file_name> <tftp_ip> on page 339
execute certificate crl export tftp <cert_name> <file_name> <tftp_ip>
execute certificate local export tftp <cert_name> <file_name> <tftp_ip> on page 339

execute certificate local generate <cert_name> <key_size> <subject> <country>
     <state> <organization> <unit> <email> on page 339
execute certificate local import tftp <file_name> <tftp_ip> on page 339
execute certificate local info <cert_name>
execute certificate local regenerate
execute certificate remote import tftp <file_name> <tftp_ip> on page 339
execute certificate remote export tftp <cert_name> <file_name> <tftp_ip> on page
     339
```

| Variable | Description | Default |
|---|---|---|
| ca import tftp <file_name> <tftp_ip> | Imports the certificate authority (CA) certificate from a TFTP server.<br>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. | |

| Variable | Description | Default |
|---|---|---|
| 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.<br>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).<br>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. | |
| local export tftp <cert_name> <file_name> <tftp_ip> | Exports a certificate signing request or a local certificate to a TFTP server.<br>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.<br>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.<br>FortiMail units require a local server certificate that it can present when clients request secure connections, including:<br>• the web UI (HTTPS connections only)<br>• webmail (HTTPS connections only)<br>• 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).<br>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 on page 196

# 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 on page 340

# 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 on page 340

# cleanqueue

Select to remove all messages from the deferred queue.

## Syntax

```
execute cleanqueue
```

## Related topics

maintain on page 355

# 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> on page 341
execute create dkim-signing-key on page 341
execute create ibe-system-key <content> on page 342
execute create resource-share on page 342
execute create system-custom-message <contents> on page 342
execute create system-favicon on page 342
execute create user-auto-forward <email_addr> <content> on page 342
execute create user-auto-reply <email_addr> <content> on page 342
execute create user-calendar <user_name>
execute create user-calendar-b64 on page 342
execute create user-calendar-tag <email_addr> <content>
execute create user-email-tag <email_addr> <content> on page 342
execute create user-filter-custom on page 342
execute create user-filter-master on page 342
execute create user-filter-sieve on page 342
execute create user-preference <user_name> <content> on page 342
execute create user-primaryaddr <user_name> <content> on page 342
execute create user-secondaryaddr <user_name> <content> on page 342
execute create user-signature <user_name> <content> on page 342
```

| Variable | Description | Default |
|---|---|---|
| custom-message <domain> <message_content> | Creates domain-wide custom messages. | |
| dkim-signing-key | Creates DomainKeys Identified Mail (DKIM) signing key. | |

| Variable | Description | Default |
|---|---|---|
| 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. | |
| 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 on page 334

# date

Use this command to set the system date.

## Syntax

```
execute date <date_str> on page 343
```

| Variable | Description | Default |
|---|---|---|
| <date_str> | Enter the system date in the format of mm/dd/yyyy. | |

## Related topics

system time manual on page 321
system time ntp on page 322

# 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 on page 344
execute db force-recover on page 344
execute db info on page 344
execute db rebuild on page 344
execute db reset <database> on page 344
execute db restore on page 344
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. | |
| 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.<br>Use the following format:<br>`execute db transfer {ftp-dump \| scp-dump \| tftp-dump} <file-name> <server-ip> <username> <password>` | |

## Related topics

maintain on page 355

# dlp

Use this command to refresh the DLP fingerprints from the fingerprint server.

## Syntax

```
execute dlp refresh <source_name> on page 344
```

| 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 on page 345
```

```
execute endpoint data backup tftp <ip_address> on page 345
execute endpoint delete <ip_address> on page 345
```

| 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 on page 365
backup on page 334

## factoryreset config

Use this command to reset the system configuration to default settings.

### Syntax

```
execute factoryreset config
```

### Related topics

backup on page 334

## 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 on page 334

# factoryreset disk

Use this command to reset the RAID level and partition disk to default settings.

## Syntax

```
execute factoryreset disk
```

## Related topics

backup on page 334

# 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 on page 334

# 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 on page 334

# 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 on page 334

# fips

Use this command to enable Federal Information Processing Standards-Common Criteria (FIPS-CC) mode.

This enhanced security mode is required by some organizations, but may not be appropriate for others. It is valid only if you have installed a FIPS-certified firmware build. For more information on FIPS, or to obtain a certified build, contact Fortinet Technical Support.

When switching to FIPS mode, you will be prompted to confirm, and must log in again.

To disable FIPS mode, restore the firmware default configuration using factoryreset on page 345.

Back up the configuration before enabling FIPS mode. When you enable or disable FIPS-CC mode, all of the existing configuration is lost. For more information on making a complete backup, see the *FortiMail Administration Guide*.

## Syntax

```
execute fips kat {3des | aes | configuration-test | integrity-test | rng | rsa |
    sha1-hmac | all} on page 349
```

| Variable | Description | Default |
|---|---|---|
| {3des \| aes \| configuration-test \| integrity-test \| rng \| rsa \| sha1-hmac \| all} | `3des`: Triple-DES known answer test.<br>`aes`: AES known answer test<br>`configuration-test`: Configuration bypass test.<br>`integrity-test`: Firmware integrity test.<br>`rng`: RNG known answer test.<br>`rsa`: RSA known answer test.<br>`sha1-hmac`: SHA1-HMAC known answer test.<br>`all`: All known answer tests. | |

## Related topics

restore image on page 367

# 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 on page 357
formatmaildisk on page 350
formatmaildisk-backup on page 351

# 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 351.

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 on page 351
formatlogdisk on page 349

# 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 350.

Regularly format the hard disk to improve performance.

## Syntax

```
execute formatmaildisk-backup
```

## Related topics

formatmaildisk on page 350
formatlogdisk on page 349

# forticloud

Use this command to manage the FortiCloud account.

## Syntax

```
execute forticloud info on page 352
execute forticloud info-apt
execute forticloud join on page 352
execute forticloud login on page 352
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:<br>• 0: Global<br>• 1: Europe<br>• 2: Japan<br>• 3: US | |
| update-apt | Force refresh of FortiCloud sandbox server addresses. | |

# ha commands

Use this command to help debugging FortiMail HA issues.

Type the full command names (such as `ha commands ...`), instead of the abbreviated names (such as `ha com ...`).

## Syntax

```
execute ha commands config-sync-start on page 353
execute ha commands config-sync-stop on page 353
execute ha commands failover-start on page 353
execute ha commands failover-stop on page 353
```

| Variable | Description | Default |
|---|---|---|
| config-sync-start | Start synchronizing the HA cluster configuration. | |
| config-sync-stop | Stop the cluster from completing synchronizing its configuration. | |
| failover-start | Allow HA failover to happen. | |
| failover-stop | Prevent HA failover form happening. | |

## Related topics

cleanqueue on page 341

# ibe data

Use this command to generate and view an IBE data file.

## Syntax

```
execute ibe data export-to-file on page 353
execute ibe data get-file-info on page 353
```

| Variable | Description | Default |
|---|---|---|
| export-to-file | Generate an IBE data file. | |
| get-file-info | Get current IBE data file information. | |

## Related topics

db on page 343

# ibe user

Use this command to maintain the expired users.

## Syntax

```
execute ibe user purge-mail <user_name> <level> on page 354
execute ibe user clean-expired-user <user_name> <level> on page 354
```

| 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 on page 343

# license

Use this command to manage the central management license.

## Syntax

```
execute license central-mgmt import tftp <ip> <file_name> on page 354
execute license central-mgmt show on page 354
```

| 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 on page 354
execute lvm enable <percentage> on page 355
execute lvm extend <percentage> on page 355
execute lvm summary on page 355
```

| Variable | Description | Default |
|---|---|---|
| disable | Stop LVM on the system. | |

| Variable | Description | Default |
|---|---|---|
| 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)<br>20 |
| 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> on page 355
```

| 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 on page 341

# 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> on page 356
```

| 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.<br><type>: optionally specify the DNS query type:<br>A -- host address<br>AAAA -- IPv6 address<br>ANY -- all cached records<br>CNAME -- canonical name<br>DLV -- DNSSEC lookaside validation<br>DNSKEY -- DNS key<br>DS -- delegation signer<br>MX -- mail exchanger<br>NS -- authoritative name server<br>NSEC -- next SECure<br>NSEC3 -- NSEC3 parameters<br>PTR -- domain name pointer<br>RRSIG -- DNSSEC signature<br>SOS -- start of authority zone<br>SPF -- sender policy framework<br>TA -- DNSSEC trust authorities<br>TXT -- text string<br>The default type is A.<br><class>: optionally specify the DNS class type: either IN or ANY.<br><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.<br><port_number>: optionally specify the port number of the DNS server. | A<br><br>ANY<br><br>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 on page 358
traceroute on page 373
system dns on page 272

# 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> on page 357
```

| 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.<br>The remaining partition (by default, 75% of the hard disk space) will be used for mail data. | 20 |

## Related topics

formatlogdisk on page 349

# 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 359.

Pings are often used to test connectivity.

## Syntax

```
execute ping {<fqdn_str> | <host_ipv4>} on page 358
```

| Variable | Description | Default |
|---|---|---|
| ping {<fqdn_str> \| <host_ipv4>} | Enter either the IP address or fully qualified domain name (FQDN) of the host. | |

## Example

This example pings a host with the IP address 172.16.1.10.

```
execute ping 172.16.1.10
```

The CLI displays the following:

```
PING 172.16.1.10 (172.16.1.10): 56 data bytes
      64 bytes from 172.16.1.10: icmp_seq=0 ttl=128 time=0.5 ms
      64 bytes from 172.16.1.10: icmp_seq=1 ttl=128 time=0.2 ms
      64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=0.2 ms
      64 bytes from 172.16.1.10: icmp_seq=3 ttl=128 time=0.2 ms
      64 bytes from 172.16.1.10: icmp_seq=4 ttl=128 time=0.2 ms
--- 172.16.1.10 ping statistics ---
      5 packets transmitted, 5 packets received, 0% packet loss
      round-trip min/avg/max = 0.2/0.2/0.5 ms
```

The results of the ping indicate that a route exists between the FortiWeb unit and 172.16.1.10. It also indicates that during the sample period, there was no packet loss, and the average response time was 0.2 milliseconds (ms).

## Example

This example pings a host with the IP address 10.0.0.1.

```
execute ping 10.0.0.1
```

The CLI displays the following:

```
PING 10.0.0.1 (10.0.0.1): 56 data bytes
```

After several seconds, no output has been displayed. The administrator halts the ping by pressing Ctrl + C. The CLI displays the following:

```
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

The results of the ping indicate that the host may be down, or that there is no route between the FortiMail unit and 10.0.0.1. To determine the cause, further diagnostic tests are required, such as traceroute on page 373.

## Related topics

ping-option on page 359
smtptest on page 371
telnettest on page 372
traceroute on page 373
system dns on page 272

# ping-option

Use this command to configure behavior of ping on page 358.

## Syntax

```
execute ping-option data-size <bytes_int> on page 359
execute ping-option df-bit {yes | no} on page 359
execute ping-option pattern <bufferpattern_hex> on page 359
execute ping-option repeat-count <repeat_int> on page 359
execute ping-option source {auto | <interface_ipv4>} on page 360
execute ping-option timeout <seconds_int> on page 360
execute ping-option tos {default | lowcost | lowdelay | reliability | throughput}
     on page 360
execute ping-option ttl <hops_int> on page 360
execute ping-option validate-reply {yes | no} on page 360
execute ping-option view-settings on page 360
```

| 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> on page 359`. | 56 |
| df-bit {yes \| no} | Enter either `yes` to set the DF bit in the IP header to prevent the ICMP packet from being fragmented, or enter `no` to allow the ICMP packet to be fragmented. | no |
| pattern <bufferpattern_hex> | Enter a hexadecimal pattern, such as `00ffaabb`, to fill the optional data buffer at the end of the ICMP packet. The size of the buffer is determined by `data-size <bytes_int> on page 359`. | |
| repeat-count <repeat_int> | Enter the number of times to repeat the ping. | 5 |

| Variable | Description | Default |
|---|---|---|
| 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:<br>• `default`: Do not indicate (that is, set the TOS byte to 0).<br>• `lowcost`: Minimize cost.<br>• `lowdelay`: Minimize delay.<br>• `reliability`: Maximize reliability.<br>• `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 on page 358
traceroute on page 373

# 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 361.

Pings are often used to test connectivity.

## Syntax

```
execute ping6 {<fqdn_str> | <host_ipv4>} on page 361
```

| 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 on page 358

ping6-option on page 361

# ping6-option

Use this command to configure behavior of ping6 on page 361.

## Syntax

```
execute ping6-option data-size <bytes_int> on page 361
execute ping6-option pattern <bufferpattern_hex> on page 362
execute ping6-option repeat-count <repeat_int> on page 362
execute ping6-option source {auto | <interface_ipv4>} on page 362
execute ping6-option timeout <seconds_int> on page 362
execute ping6-option tos {default | lowcost | lowdelay | reliability | throughput}
     on page 362
execute ping6-option ttl <hops_int> on page 362
execute ping6-option validate-reply {yes | no} on page 362
execute ping6-option view-settings on page 362
```

| 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> on page 362`. | 56 |

| Variable | Description | Default |
|---|---|---|
| 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>` on page 361. | |
| 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:<br>• `default`: Do not indicate (that is, set the TOS byte to 0).<br>• `lowcost`: Minimize cost.<br>• `lowdelay`: Minimize delay.<br>• `reliability`: Maximize reliability.<br>• `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 on page 358
ping6 on page 361
db on page 343

# 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 on page 379

# 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 on page 370

# 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 on page 363
restore config on page 365
restore image on page 367

# restore as

Use this command to restore an antispam configuration file from a TFTP server.

## Syntax

```
execute restore as tftp <filename_str> on page 365 <server_ipv4> on page 365
```

| 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 on page 365

# restore av

use this command to restore an antivirus configuration file from a TFTP server.

## Syntax

```
execute restore av tftp <filename_str> on page 365 <server_ipv4> on page 365
```

| 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 on page 364

# 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> on page 366 <server_ipv4> on page 366 |
    management-station {normal | template} on page 366 <revision_int> on page
    366}
```

| 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:<br>• `normal`: Restore a configuration revision number.<br>• `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 on page 334

system central-management

# restore image

Use this command to restore a firmware file from an FTP, SCP, 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> on page 367 <server_ipv4> on page
    367 <user><password> on page 367
```

| Variable | Description | Default |
|---|---|---|
| <filename_str> | Enter the name of the firmware file backup file. | |
| <server_ipv4> | Enter the IP address of the server. | |
| <user><password> | You may need to enter the credentials to log on to the server. | |

## 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 on page 365

system central-management

# 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> on page 368 <server_ipv4> on page
    368}
```

| 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 on page 365

# safelist

Use this command to configure safelist operations.

## Syntax

```
execute safelist add
execute safelist backup
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):<br>`execute safelist add [domain \| user] <domain-name \| user-name> <list-content>`<br>`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):<br>`execute safelist backup [domain \| user] <domain-name \| user-name> <tftp-server-ip> <file-name>`<br>`execute safelist backup [system] <tftp-server-ip> <file-name>` | |
| purge | Purge a domain or user level safelist, or system level safelist, as shown below (respectively):<br>`execute safelist purge [domain \| user] <domain-name-list \| user-name-list>`<br>`execute safelist purge [system]` | |
| remove | Remove a domain or user level safelist, or system level safelist, as shown below (respectively):<br>`execute safelist remove [domain \| user] <domain-name \| user-name> <list-content>`<br>`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):<br>`execute safelist restore [domain \| user] <domain-name \| user-name> <tftp-server-ip> <file-name>`<br>`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 on page 363

# smtptest

Use this command to test SMTP connectivity to a specified host.

## Syntax

```
execute smtptest {<fqdn_str> | <host_ipv4>} on page 371[:<port_int>] on page 371
    [domain <domain_str>] on page 371
```

| 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 on page 372
traceroute on page 373
ping on page 358
system dns on page 272

# ssh

Use this command to connect to another device via SSH.

## Syntax

```
execute ssh <username@host> <password> on page 372
```

| 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 on page 372
execute storage fscheck on page 372
execute storage start on page 372
execute storage test on page 372
```

| 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>} on page 372[:<port_int>] on page 372
```

| 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 on page 371
traceroute on page 373
ping on page 358
system dns on page 272

# 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>} on page 373
```

| 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 272.

## Related topics

smtptest on page 371
telnettest on page 372
ping on page 358
ping-option on page 359
system dns on page 272

# 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 278 and system fortiguard antispam on page 280.

## Syntax

```
execute update {as | av | now}
```

## Related topics

system fortiguard antivirus on page 278

system fortiguard antispam on page 280

# 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 on page 334.

## Syntax

```
execute user-config generate on page 375
execute user-config getinfo on page 375
```

| 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 on page 334

# vm

Use this command to upload a VM license.

## Syntax

```
execute vm license tftp <license_file_name> <tftp_server_ip> on page 376
```

| Variable | Description | Default |
| --- | --- | --- |
| <license_file_name> <tftp_server_ip> | Specify the license file name and the TFTP server IP address. | |

# 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` on page 378, are used to display system information that is **not** configurable. This chapter describes this type of `get` command.

This chapter describes the following commands:



Although not explicitly shown in this section, for all `config` on page 40 commands, there are related `get` and `show & show full-configuration` on page 381 commands which display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see config on page 40.

# 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 on page 379

# system status

Use this command to display FortiMail system status information including:

- firmware version, build number and date
- antivirus definition version and release date and time
- FortiMail unit serial number and BIOS version
- log hard disk availability
- mailbox disk availability
- host name
- operation mode
- distribution scope
- branching point (same as firmware build number)
- release version
- certificate bundle
- system time

## Syntax

```
get system status
```

## Example

```
Version: FortiMail-VM-KVM v7.0.1(GA), build159, 2021.08.31
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 configured mode: Off
HA effective mode: Off
FIPS-CC status: disabled
Strong-crypto: enabled
Distribution: International
Branch point: 159
Virus DB: 88.00819(2021-09-02 08:39)
Extended DB: Disabled
Extreme DB: Disabled
AntiSpam DB: 7.00453(2021-08-30 20:47)
GeoIP DB: 2.00088(2021-07-20 21:29)
Certificate Bundle: 1.00026(2021-05-25 11:30)
Uptime: 0 days 22 hours 42 minutes
Last reboot: Wed Sep 01 12:21:59 PDT 2021
```

```
System time: Thu Sep 02 11:04:31 PDT 2021
```

## Related topics

system performance on page 378

# 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` on page 40 commands, there are related `get` on page 377 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, simliar 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.

www.fortinet.com