FortiAnalyzer™

Version 4.0 MR2
CLI Reference

FORTINET®

FortiAnalyzer CLI Reference

Version 4.0 MR2

11 January 2011

Revision 5

Trademarks

Regulatory compliance

FCC Class A Part 15 CSA/CUS

Contents

Introduction

FortiAnalyzer units are network appliances that provide integrated log collection, analysis tools and data storage. Detailed log reports provide historical as well as current analysis of network traffic, such as email, FTP and web browsing activity, to help identify security issues and reduce network misuse and abuse.

This document describes how to use the FortiAnalyzer Command Line Interface (CLI).

This section describes:

- Registering your Fortinet product
- Customer service and technical support
- Training
- Documentation
- Conventions

Note: Diagnose commands are also available from the FortiAnalyzer CLI. These commands are used for gathering detailed information useful to Fortinet technical support for debugging; because diagnose commands are not a part of normal product use, diagnose commands are not covered in this document. Contact Fortinet technical support before using diagnose commands.

Registering your Fortinet product

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

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

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

Customer service and technical support

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

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

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

Training

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

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

Documentation

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

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

Fortinet Tools and Documentation CD

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

Fortinet Knowledge Base

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

Comments on Fortinet technical documentation

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

Conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

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

Notes, Tips and Cautions

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

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

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

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

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

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

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

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

Emphasis	HTTP connections are ***not*** secure and can be intercepted by a third party.

File content	`<HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD>`
	`<BODY><H4>You must authenticate to use this service.</H4>`

Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com.
Keyboard entry	Type a name for the remote VPN peer or client, such as `Central_Office_1`.
Navigation	Go to *VPN > IPSEC > Auto Key (IKE)*.
Publication	For details, see the *FortiGate Administration Guide*.

What's new

The tables below list commands which have changed since the previous release, FortiAnalyzer 4.0 MR1.

Command	Change

`config system global`
`  set ediscovery-quota <number>`
	New command to set the disk quota for eDiscovery file usage.

`config system migration`
`  set e-discovery {enable | disable}`
	New command to enable/disable eDiscovery file migration.

`config system sql`	New command to configure the SQL database options.
`config sql-report chart`	New command to configure a customized chart or edit an existing chart for your reports.
`config sql-report dashboard`	New command to configure the report dashboard that you can view under *Report* > *Access* on the web-based manager.
`config sql-report dashboard-tab`	New command to add a report dashboard or edit the name of an existing dashboard that you can view under *Report* > *Access* on the web-based manager.
`config sql-report dataset`	New command to configure datasets that will be used in "config sql-report chart" on page 75. A dataset must be configure first, before configuring a chart, because the chart must contain a dataset.
`config sql-report layout`	New command to configure the layout for the report to be generated. The report layout includes charts, devices, titles, headers and footers, if applicable.
`execute backup ediscovery {all | <folder_name>} {ftp | scp | sftp | tftp} <server_ipv4> <username_str> <password_str> <directory_str> <file_name>`	New command to back up eDiscovery files.
`execute reset-sqllog-transfer`	New command to send logs received by the FortiAnalyzer unit to the SQL database for generating reports.
`execute sql-local {remove-db | remove-device <device_ID> | remove-logtype <log_type>}`	New commands to remove logs from the local SQL database.
`execute sql-query-dataset <dataset_name> <device/group_name> <vdom>`	New command to test the SQL dataset query.
`execute sql-query-generic <sql_statement>`	New command to run SQL query statements.

Using the CLI

This section explains how to connect to the CLI and describes the basics of using the CLI. You can use CLI commands to view all system information and to change all system configuration settings.

This section describes:

- Connecting to the CLI
- Command syntax
- Sub-commands
- Permissions
- Tips and Tricks

Connecting to the CLI

You can access the CLI in a variety of ways, by the CLI console widget located on the Dashboard page of the web-based manager, locally, or through the network. Local access is when you connect your management computer directly to your FortiAnalyzer unit's console port. Network access is when you remotely access the CLI suing SSH or Telnet client software. Connecting to the console or network connection varies by FortiAnalyzer model. For example, a FortiAnalyzer-2000 unit connects using a RJ-45 to DB-9 cable, but a FortiAnalyzer-2000A unit connects using a null-modem cable. See the *FortiAnalyzer Install Guide* to verify which cable is correct for your FortiAnalyzer model.

Local access is required if:

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

Before accessing the CLI through the network, you need to enable SSH or Telnet (or both if required) on the network interface that users will be accessing the CLI through.

This topic contains the following:

- Connecting to the console
- Enabling access to the CLI through the network (SSH or Telnet)
- Connecting to the CLI using SSH
- Connecting to the CLI using Telnet

Connecting to the console

When connecting to the console, you need:

- a computer with an available serial (communications) port
- a null modem cable or RJ-45 to DB-9 cable (whichever is correct for your FortiAnalyzer model).

- terminal emulation software, such as HyperTerminal for Windows.

See your *FortiAnalyzer Install Guide* to verify which cable is correct for your FortiAnalyzer model.

The following procedure describes a console connection using terminal emulator Windows HyperTerminal; steps may vary with other terminal emulators.

To connect to the console of a FortiAnalyzer unit

1 Connect the FortiAnalyzer unit’s console port to the communications port on your management computer using the null modem or RJ-45 to DB-9 cable.

2 Verify that the FortiAnalyzer unit is powered on.

3 On your management computer, start HyperTerminal.

4 Cancel any dialogs requesting phone or modem information, such as area codes or tone dialing.

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

6 Cancel any dialogs requesting phone or modem information such as area codes or tone dialing.

7 On Connect To, from Connect using, select the communications port where you connected the FortiAnalyzer unit.

This is usually COM1 for DB-9 cable connections, and TCP/IP for RJ-45 cable connections.

8 Select *OK*.

9 Select the following in *Port Settings* and then select *OK*.

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

10 Press Enter to connect to the FortiAnalyzer CLI.

A prompt appears.

11 Type a valid administrator name and press Enter.

12 Type the password for this administrator and press Enter.

You can now enter CLI commands.

Note: If too many incorrect login or password attempts occur in a row, you will be disconnected. You must reconnect to attempt the login again.

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

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

SSH or Telnet access to the CLI is formed by connecting your computer to the FortiAnalyzer unit using the null-modem or RJ-45 to DB-9 cable (whichever is correct for your FortiAnalyzer model). You can either connect directly, which uses a peer connection between the two, or through any intermediary network.

You must enable Secuire Shell (SSH) 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 FortiAnalyzer unit with a static route to a router that can forward packets from the FortiAnalyzer unit to your computer.

Network CLI access may be configured using either the CLI or the web-based manager.

- To configure CLI access using the web-based manager, see the “Configuring” chapter in the *FortiAnalyzer Administration Guide*.
- To configure CLI access using the CLI, use the following procedure.

To use the CLI to configure SSH or Telnet access

1. Establish a console or network connection to the CLI.
2. Log in to the CLI.
3. Enter the command to configure an interface to accept either SSH or Telnet administrative connections.

   For example, to allow both SSH and Telnet on `port1`:

   ```
   config system interface
     edit port1
       set allowaccess ssh telnet
   end
   ```
4. Press Enter at the end of each command. Type `end` and press Enter to save the changes to the FortiAnalyzer configuration.
5. To confirm the configuration, enter the command to view the access settings for the interface.

   ```
   get system interface
   ```

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

Connecting to the CLI using SSH

After configuring the FortiAnalyzer unit to accept SSH connections, you can use an SSH client on your management computer to connect to the FortiAnalyzer CLI.

SSH provides both secure authentication and secure communications to the FortiAnalyzer CLI from your internal network or the Internet.

To connect to the CLI using SSH

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

   The FortiAnalyzer model name followed by a `#` is displayed:

   ```
   FortiAnalyzer-400 #
   ```

   You can now enter CLI commands.

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

If four incorrect login or password attempts occur in a row, you will be disconnected. Reconnect to attempt the login again.

Connecting to the CLI using Telnet

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

After configuring the FortiAnalyzer unit to accept Telnet connections, you can use a Telnet client on your management computer to connect to the FortiAnalyzer CLI.

To connect to the CLI using Telnet

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

   The FortiAnalyzer model name followed by a `#` is displayed:

   ```
   FortiAnalyzer-400 #
   ```

   You can now enter CLI commands.

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

Command syntax

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

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

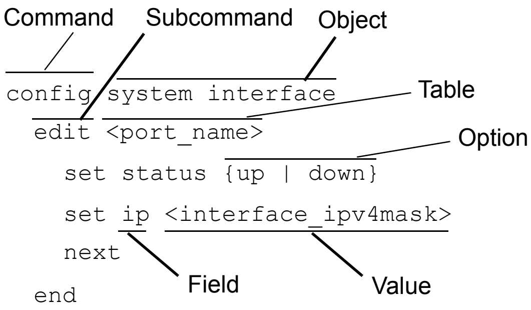
Terminology

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

```
get system admin
```

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

Figure 1: Command syntax terminology



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

- **command –** A word that begins the command line and indicates an action that the FortiAnalyzer 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.

  Valid command lines must be unambiguous, if abbreviated. Optional words or other command line permutations are indicated by syntax notation.
- **sub-command –** A kind of command that is available only when nested within the scope of another command. After entering a command, its applicable sub-commands are available to you until you exit the scope of the command, or until you descend an additional level into another sub-command. Indentation is used to indicate levels of nest 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.
- **table –** A set of fields that is one of possible multiple similar sets which each have a name or number, such as administrator account, policy or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them.
- **field –** A 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 FortiAnalyzer 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.
- **option –** A kind of value that must be one or more words of a fixed set of options.

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
```

Notation

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

Table 2: Command syntax notation

Convention	Description

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

Angle brackets `< >`	A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example: `<retries_int>` indicates that you should enter a number of retries, such as `5`. Data types include: • `<xxx_name>`: A name referring to another part of the configuration, such as `policy_A`. • `<xxx_index>`: An index number referring to another part of the configuration, such as `0` for the first static route. • `<xxx_pattern>`: A regular expression or word with wild cards that matches possible variations, such as `*@example.com` to match all email addresses ending in `@example.com`. • `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`. • `<xxx_email>`: An email address, such as `admin@mail.example.com`. • `<xxx_url>`: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as `http://www.fortinet./com/`. • `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`. • `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`. • `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`. • `<xxx_ipv4/mask>`: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as such as `192.168.1.99/24`. • `<xxx_ipv4range`>: A hyphen (`-`)-delimited inclusive range of IPv4 addresses, such as `192.168.1.1-192.168.1.255`. • `<xxx_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 25. • `<xxx_int>`: An integer number that is ***not*** another data type, such as `15` for the number of minutes.
Curly braces `{ }`	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].

Table 2: Command syntax notation

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

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

Sub-commands

After connecting to the CLI, you can enter the commands. Each command line consists of a command word that is usually followed by words for the configuration data or other specific items that the command uses or affects. For example,

```
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
  end
```

Sub-command scope is indicated in the document by indentation. For more information, see “Indentation” on page 19.

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

- commands affecting fields
- commands affecting tables

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

Table 3: Commands for tables

delete <table>	Remove a table from the current object. For example, in `config system admin`, you could delete an administrator account named `newadmin` by typing `delete newadmin` and pressing Enter. This deletes `newadmin` and all its fields, such as `newadmin`'s `name` and `email-address`. `delete` is only available within objects containing tables.
edit <table>	Create or edit a table in the current object. For example, in `config system admin`: • edit the settings for the default `admin` administrator account by typing `edit admin`. • add a new administrator account with the name `newadmin` and edit `newadmin`'s settings by typing `edit newadmin`. `edit` is an interactive sub-command: further sub-commands are available from within `edit`. `edit` changes the prompt to reflect the table you are currently editing. `edit` is only available within objects containing tables.
end	Save the changes to the current object and exit the `config` command. This returns you to the top-level command prompt.
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values.
purge	Remove all tables in the current object. For example, in `config forensic user`, you could type `get` to see the list of user names, then type `purge` and then `y` to confirm that you want to delete all users. `purge` is only available for objects containing tables. **Caution:** Back up the FortiAnalyzer unit before performing a `purge`. `purge` cannot be undone. To restore purged tables, the configuration must be restored from a backup. For details, see "execute backup" on page 125. **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 FortiAnalyzer unit to be formatted and restored.
rename <table> to <table>	Rename a table. For example, in `config system admin`, you could rename `admin3` to `fwadmin` by typing `rename admin3 to fwadmin`. `rename` is only available within objects containing tables.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.

Example of table commands

From within the system admin object, you enter:

```
edit admin_1
```

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

```
new entry 'admin_1' added
[admin_1] #
```

Table 4: Commands for fields

`abort`	Exit both the `edit` and/or `config` commands without saving the fields.
`end`	Save the changes made to the current table or object fields, and exit the `config` command. (To exit without saving, use `abort` instead.)
get	List the configuration of the current object or table. • In objects, `get` lists the table names (if present), or fields and their values. • In a table, `get` lists the fields and their values.
`next`	Save the changes you have made in the current table's fields, and exit the `edit` command to the object prompt. (To save and exit completely to the root prompt, use `end` instead.) `next` is useful when you want to create or edit several tables in the same object, without leaving and re-entering the `config` command each time. `next` is only available from a table prompt; it is not available from an object prompt.

**`set <field>`
`<value>`**
	Set a field's value.
	For example, in `config system admin`, after typing `edit admin`, you could type `set passwd newpass` to change the password of the `admin` administrator to `newpass`.
	Note: When using `set` to change a field containing a space-delimited list, type the whole new list. For example, `set <field> <new-value>` will replace the list with the `<new-value>` rather than appending `<new-value>` to the list.

show	Display changes to the default configuration. Changes are listed in the form of configuration commands.

**`unset`
`<field>`**
	Reset the table or object's fields to default values.
	For example, in `config system admin`, after typing `edit admin`, typing `unset passwd` resets the password of the `admin` administrator account to the default (in this case, no password).

Example of field commands

From within the admin_1 table, you enter:

```
set passwd my1stExamplePassword
```

to assign the value `my1stExamplePassword` to the passwd field. If you wanted to edit the next administrator's table, you would enter the `next` command to save the changes and edit the next administrator's table.

Permissions

Caution: Set a strong password for the admin administrator account, and change the password regularly. By default, this administrator account has no password. If you do not change this administrator's account password on a regular basis, it may compromise the security of your FortiAnalyzer unit.

Depending on the account that you use to log in to the FortiAnalyzer unit, you may not have completed access to all CLI commands.

There are three possible permission types for an administrator account:

- Administrator (also known as "super")
- Read & Write
- Read Only

The permissions of an administrator account, combined with whether the administrator account is assigned to a specific protected domain, such as example.com, or is assigned to the entire system, will determine the parts of the configuration that the administrator is permitted to modify and/or view.

Table 5: Administrator account permission by domain assignment

Permissions	Domain: system	Domain: adom_1.com
Administrator	• Can create, view and change all other administrator accounts, except the admin administrator account • Can view and change all parts of the FortiAnalyzer unit's configuration, including uploading configuration backup files, and restoring firmware default settings. • Can release and delete quarantined email messages for all protected domains • Can back up and restore databases • Can manually update firmware and vulnerability management definitions • Can restart and shut down the FortiAnalyzer unit.	• Can create, view and change other administrator accounts with Read & Write and Read Only permissions in its own protected domain. • Can only view and change settings, including profiles and policies, in its own protected domain. • Can only view profiles and policies created by an administrator whose Domain is system • Can be only one per protected domain.
Read & Write	• Can only view and change its own administrator account • Can view and change parts of the FortiAnalyzer unit's configuration at the system and protected domain levels. • Can release and delete quarantined email messages for all protected domains. • Can back up and restore databases.	• Can only view and change its own administrator account • Can only view and change parts of the FortiAnalyzer unit's configuration in its own protected domain • Can only view profiles and policies created by an administrator whose Domain is system. • Can release and delete quarantined email messages in its own protected domain.
Read Only	• Can only view and change its own administrator account. • Can view the FortiAnalyzer unit configuration at the system and protected domain levels • Can release and delete quarantined email messages for all protected domains • Can back up databases	• Can only view and change it's own administrator account • Can only view settings in its own protected domain • Can only view profiles and policies created by an administrator whose Domain is system.

Unlike other administrator accounts whose permission is Administrator and Domain is system, the administrator account named admin exists by default and cannot be deleted. The admin administrator account is similar to a root administrator account. This administrator account always has full permissions to view and change all FortiAnalyzer 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. Its name, permissions, and assignment to the system domain cannot be changed.

Tips and Tricks

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

This topic includes the following:

- Help
- Shortcuts and key commands
- Command abbreviation

Help

To display 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

The following table explains the available shortcuts and key commands that you can use during entry of commands.

Table 6: Shortcuts and key commands

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

Command abbreviation

You can abbreviate command words to the smallest number of non-ambiguous characters. For example, the command `get system status` could be abbreviated to `g sys st`.

Special characters

The characters <, >, (,), #, ‘ , and “ are not permitted in most CLI fields.

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 character (blackslash).

Table 7: Entering special characters

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

Language support

Characters such as n, e, 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 CLI will not accept most symbols and other encoded characters as input when configuring the host name. This means that languages other than English often cannot be used; however, dictionary profiles support terms encoded in UTF-8, and therefore support a number of languages.

It is best to use only ASCII characters when configuring the FortiAnalyzer unit using the web-based manager or CLI. By using only ASCII, you do not need to worry about:

- web browser language support
- Telnet and/or SSH client support
- font availability
- compatibility of your input’s encoding with the encoding/language setting of the web-based manager
- switching input methods when entering a command word such as get in ASCII but a setting that uses a different encoding.

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

Baud rate

You can change the default console connection baud rate.

Editing the configuration file on an external host

Caution: Do not edit the first line. The first line or lines of the configuration file (preceded by an # character) contains information about the firmware version and FortiAnalyzer models. If you changed the model number, the FortiAnalyzer unit will reject the configuration file when you attempt to restore it.

You can edit the FortiAnalyzer 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 FortiAnalyzer unit.

To edit the configuration on your computer

1 Use `execute backup config` (“execute backup” on page 125) to download the configuration file to a TFTP server, such as your management computer.

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

3 Use `execute restore config` (“execute restore” on page 134) to upload the modified configuration file back to the FortiAnalyzer unit.

The FortiAnalyzer unit downloads the configuration file and checks that the model information is correct. If it is, the FortiAnalyzer unit loads the configuration file and checks each command for errors. If the configuration file is somehow invalid, an error message is displayed and the configuration file is rejected. If the configuration file is valid, the FortiAnalyzer unit restarts and loads the new configuration.

Working with Administrative Domains

Administrative Domains (ADOMs) enable the `admin` administrator to constrain other FortiAnalyzer unit administrators' access privileges to a subset of devices in the device list. For FortiGate devices with virtual domains (VDOMs), ADOMs can further restrict access to only data from a specific FortiGate VDOM.

This section contains the following topics:

- About administrative domains (ADOMs)
- Configuring ADOMs
- Accessing ADOMs as the admin administrator
- Assigning administrators to an ADOM

About administrative domains (ADOMs)

Enabling ADOMs alters the structure and available functionality of the web-based manager and CLI according to whether you are logging in as the `admin` administrator, and, if you are not logging in as the `admin` administrator, the administrator account's assigned access profile.

Note: ADOMs are not available on the FortiAnalyzer-100/100A/100B.

Note: The `admin` administrator can further restrict other administrators' access to specific configuration areas within their ADOM by using access profiles. For more information, see "accprofile" on page 86.

Table 8: Characteristics of the CLI and web-based manager when ADOMs are enabled

	`admin` **administrator account**	**Other administrators**
Access to `config global`	Yes	No
Access to `config adom devices` **(can create ADOMs)**	Yes	No
Can create administrator accounts	Yes	No
Can enter all ADOMs	Yes	No

Table 9: Command locations when ADOMs are enabled

Within Global Configuration (`config global`**):**	**Within each ADOM:**
`config system global`	`config system ip-alias`
`config system interface`	`config system ldap`
`config system ip-alias`	`config system mail`
`config system dns`	`config report output`
`config system accprofile`	`config report filter`
`config system radius`	`config report layout`
`config system ldap`	`config report schedule`
`config system authgrp`	`config adom devices` (only available when logged in as `admin` administrator)
`config system console`	`config adom virtual-domains` (only available when logged in as `admin` administrator)
`config system route`	`config adom email-domains` (only available when logged in as `admin` administrator)
`config system raid`	`config log device-group`
`config system admin`	
`config system snmp`	
`config system syslog`	
`config system mail`	
`config system event`	
`config system alert_console`	
`config system auto-delete`	
`config system fortiguard`	
`config report language`	
`config report output`	
`config report filter`	`execute content_files`
`config report layout`	`execute quarantine_files`
`config report schedule`	`execute ips-pkt`
`config nas protocol`	`execute column-settings`
`config nas user`	
`config nas group`	
`config nas share`	
`config nas nfs`	
`config log device` (devices assigned to an ADOM other than root cannot be deleted)	
`config log device-group`	
`config log unregistered`	
`config log settings`	
`config log aggregration`	
`config log forwarding`	
`config backup schedule`	

Table 9: Command locations when ADOMs are enabled

`config vm sensor`
`config vm scan-profile`
`config vm host-asset`
`config vm asset-group`
`config vm map-config`
`config vm schedule`
`config vm business-risk`
`config gui console`
`execute reboot`
`execute shutdown`
`execute reload`
`execute restore`
`execute backup`
`execute import`
`execute import-lang`
`execute formatlogdisk`
`execute factoryreset`
`execute ping`
`execute ping-options`
`execute disconnect`
`execute set-time`
`execute set-date`
`execute traceroute`
`execute vm`
`execute update-vm`
`execute content-files`
`execute quarantine_files`
`execute ips-pkt`
`execute admin-cert`
`execute column-settings`
`execute run (arg)`

- If ADOMs are enabled and you log in as `admin`, a superset of the typical CLI commands appear, allowing unrestricted access and ADOM configuration.
  - `config global` contains settings used by the FortiAnalyzer unit itself and settings shared by ADOMs, such as the device list, RAID, and administrator accounts. It does not include ADOM-specific settings or data, such as logs and reports. When configuring other administrator accounts, an additional option appears allowing you to restrict other administrators to an ADOM.
  - `config adom` allows you to configure or access ADOMs. You can add a device to one or more ADOMs. If you enter an ADOM, a Main Menu item appears in the menu, enabling you to return to the top level menu area, Administrative Domain Configuration.

- If ADOMs are enabled and you log in as any other administrator, you enter the ADOM assigned to your account. A subset of the typical menus or CLI commands appear, allowing access only to only logs, reports, quarantine files, content archives, IP aliases, and LDAP queries specific to your ADOM. You cannot access Global Configuration, or enter other ADOMs.

  By default, administrator accounts other than the `admin` account are assigned to the `root` ADOM, which includes all devices in the device list. By creating ADOMs that contain a subset of devices in the device list, and assigning them to administrator accounts, you can restrict other administrator accounts to a subset of the FortiAnalyzer unit's total devices or VDOMs.

The `admin` administrator account cannot be restricted to an ADOM. Other administrators are restricted to their ADOM, and cannot configure ADOMs or Global Configuration.

The maximum number of ADOMs varies by FortiAnalyzer model.

FortiAnalyzer Model	**Number of Administrative Domains**
FortiAnalyzer-400	10
FortiAnalyzer-800/800B	50
FortiAnalyzer-2000/2000A	100
FortiAnalyzer-4000/4000A	250

Configuring ADOMs

Administrative domains (ADOMs) are disabled by default. When enabled, there is initially only one ADOM, the `root` ADOM, that all devices belong to. All existing administrator accounts except the `admin` account are assigned to the `root` ADOM. To restrict administrators to a subset of devices or virtual domains (VDOMs), you must first create ADOMs, then assign administrator accounts to the new ADOMs.

To disable ADOMs, you must first delete all ADOMs except the `root` ADOM. Disabling the administrative domains feature then removes any administrator accounts associated with ADOMs other than the `root` ADOM. If you do not wish to delete those administrator accounts, assign them to the `root` ADOM before disabling ADOMs.

Note: ADOMs are not available on the FortiAnalyzer-100/100A/100B.

Caution: Enabling ADOMs moves non-global configuration items to the `root` ADOM. Back up the FortiAnalyzer unit configuration before beginning this procedure. For more information, see "execute backup" on page 125.

To enable ADOMs

1. Log in as `admin`.

   Other administrators cannot enable, disable, or configure ADOMs.

2. Enter the following commands:

```
config system global
  set adom enable

end
```

```
exit
```

3. To confirm that ADOMs are enabled, log in again as `admin` and enter:

   ```
   config ?
   ```

   These top-level objects appear:

   - `global`
   - `adom`

   To create ADOMs, see “To add an ADOM” on page 33. To assign an administrator to an ADOM, see “Assigning administrators to an ADOM” on page 35.

To add an ADOM

1. Log in as `admin`.

   Other administrators cannot enable, disable, or configure ADOMs.

2. Add the ADOM and define which devices belong to that ADOM.

   For example, where the name of the ADOM is `<adom_str>` and a name of a device in the global device list is `<device_str>`, enter the following commands:

   ```
   config adom
      edit <adom_str>
         config adom devices
            edit <device_str>
         end
      end
   ```

If the ADOM should contain multiple devices, enter the command `edit <device_str>` once for each device.

3. To confirm that the ADOM contains the correct devices, enter:

   For example, where the name of the ADOM is `<adom_str>`, enter the following commands:

   ```
   config adom
      edit <adom_str>
         show adom devices
      end
   ```

   A list of devices belonging to the ADOM appears.

Caution: Deleting ADOMs, which can occur when disabling the ADOM feature, removes administrator accounts assigned to ADOMs other than the `root` ADOM. Back up the FortiAnalyzer unit configuration before beginning this procedure. For more information, see “execute backup” on page 125.

To disable ADOMs

1. Log in as `admin`.

   Other administrators cannot enable, disable, or configure ADOMs.

2. Enter the command `config adom`, then delete all ADOMs other than the `root` ADOM.

   For example, if you have the ADOMs `root`, `adom_a` and `adom_b`, you would enter these commands:

```
config adom
   delete adom_a
   delete adom_b

end
```

If any other ADOMs except the `root` ADOM remain, the command to disable ADOMs will not succeed.

3 Enter the following commands:

```
config global

  config system global
    set adom disable
  end

end

exit
```

4 To confirm that ADOMs are disabled, log in again as `admin` and enter:

```
config ?
```

These top-level objects appear:

- `system`
- `report`
- `nas`
- `log`
- `backup`
- `vm`
- `gui`

Accessing ADOMs as the admin administrator

When ADOMs are enabled, additional ADOM commands become available to the `admin` administrator and the structure of the CLI changes. After logging in, other administrators implicitly access the subset of the CLI tree that pertains only to their ADOM, while the `admin` administrator accesses the root of the CLI tree and can use all commands. To configure items specific to an ADOM, the `admin` administrator must explicitly enter the part of the CLI tree that contains an ADOM's table.

To access an ADOM

1 Log in as `admin`.

Other administrators cannot access ADOMs other than the one assigned to their account.

2 Enter the ADOM's table.

For example, where the name of the ADOM is `<adom_str>`, enter the following commands:

```
config adom

  edit <adom_str>
```

3 You can now configure settings specific to that ADOM. To confirm that you are configuring an ADOM and not global settings, enter:

```
config ?
```

These top-level objects appear:

- `system`
- `report`
- `log`
- `adom`

Assigning administrators to an ADOM

The `admin` administrator can create other administrators and assign an ADOM to their account, constraining them to configurations and data that apply only to devices in their ADOM.

For example, you could create an administrator `example_admin` that is constrained to configurations and data applicable to the administrative domain `ADOM_A`.

```
config global
  config system admin
  edit example_admin
    set accprofile prof_admin
    set password sw0rdf1sh
    set adom ADOM_A
  end
end
```

Note: By default, when ADOMs are enabled, existing administrator accounts other than `admin` are assigned to the `root` ADOM, which contains all devices in the device list. For more information about creating other ADOMs, see "Configuring ADOMs" on page 32.

config

Use the `config` commands to modify the FortiAnalyzer configurations.

This chapter describes the following `config` commands:

backup schedule

Use this command to configure a schedule of when to back up the configuration file.

Syntax

```
config backup schedule
  config configuration
    set dir <remoteserver_directory>
    set ip <ipv4>
    set password <psswrd>
    set schedule {enable | disable}
    set service {ftp | tftp | scp | sftp}
    set time <hh:mm>
    set type {daily | dates <value> | days [fri mon sat sun thu tue wed]}
    set user <user_name>
end
```

Keywords and variables	Description	Default
`dir <remoteserver_directory>`	Enter the directory path of the remote directory server on the backup server. If you want the backup to upload to the home directory, use “.”.	No default
`ip <ipv4>`	Enter the IP address of the backup server.	`0.0.0.0`
`password <psswrd>`	Enter the password of the backup server.	No default
`schedule {enable | disable}`	Enable the scheduled backup of the configuration.	`disable`
`service {ftp | tftp | scp | sftp}`	Enter the type of upload server.	`ftp`
`time <hh:mm>`	Enter the time of day to upload the backup. Use the hh:mm format and make sure to use the 24-hour format when entering pm time, such as 2 p.m. which would be 14:00.	`00:00`
`type {daily | dates <value> | days [fri mon sat sun thu tue wed]}`	Enter when the backup will occur, such as on a daily basis or during a specific day of the week. You can also choose to schedule the backup on a specific day of the month, such as 31 or the 31st day of the month. For multiple dates or days of the week, use a space between each number or day of week, for example, 1 12 31.	`daily`
`user <user_name>`	Enter the remote user’s identification name that is used to log in to the backup server.	No default

Example

In this example, the scheduled backup for the configuration is to the home directory of a remote computer.

```
config backup schedule
  config configuration
    set dir d:\scheduled_backups
    set ip 172.16.155.122
    set password p8assw0rd
    set schedule enable
    set service tftp
    set time 08:30
    set type days mon tue fri
    user user_1
  end
```

History

4.0 MR1	New.

gui console

Use this command to configure the web-based manager CLI console.

Syntax

```
config gui console
  set preferences <filedata>
end
```

Keywords and variables	Description	Default
`preferences <filedata>`	Upload the base-64 encoded file that contains the commands to set up the web-based manager CLI console.	No default

Example

This example shows how to upload the data file `pref-file` containing commands to set up the web-based manager CLI console.

```
config gui console
  set preferences pref-file
end
```

History

3.0 MR7	New.

gui preferences

Use this command to show or hide some functions on the web-based manager.

Syntax

```
config gui preferences
   set <gui_item> {disable | enable}
end
```

Keywords and variables	Description	Default
`<gui_item> {disable	enable}`	Hide or show the 14 GUI menus on the web based manager. These GUI menus/functions are not commonly used and are thus hidden by default.	`disable`

History

3.0 MR7	New.

log aggregation

Use this command to enable log aggregation and configure the server IP address.

Syntax

```
config log aggregation
   set aggregation_time <hour_int>
   set mode {client | disabled | server }
   set password <password_str>
   set server_ip <ip_address>
end
```

Keywords and variables	Description	Default
`aggregation_time <hour_int>`	Enter the hour of the day when the FortiAnalyzer unit sends logs to the log aggregation server. The range is 0-23. This option appears only if `mode` is `client`.	`0`
`mode {client | disabled | server }`	Select to enable log aggregation in either client or server mode, or to disable log aggregation. **Note**: The `server` option does not appear on FortiAnalyzer-100A models.	`disabled`
`password <password_str>`	Enter the password of the log aggregation server. • If `mode` is `server`, clients connecting to this FortiAnalyzer unit must match this configured password. • If `mode` is `client`, the FortiAnalyzer unit uses this password when connecting to its log aggregation server. This option appears only if `mode` is `client` or `server`.	No default.
`server_ip <ip_address>`	Enter the IP address of the log aggregation server. This option appears only if `mode` is `client`.	No default.

Example

The following example configures the FortiAnalyzer unit as an aggregation client that send logs to an aggregation server daily at 10 AM.

```
config log aggregation
  set mode client
  set server_ip 10.10.35.99
  set password **********
  set aggregation_time 10
end
```

History

3.0 MR2	New group of keywords and commands.

log device

Caution: Changing the FortiGate unit's FortiAnalyzer settings clears sessions to its FortiAnalyzer unit's IP address. If the FortiAnalyzer unit is behind a NAT device, this also resets sessions to other devices behind that same NAT.

To prevent disruption of other devices' traffic, on the NAT device, create a separate virtual IP for the FortiAnalyzer unit.

Use this command to add and configure a device connected to the FortiAnalyzer unit, and how the FortiAnalyzer unit interacts with the device.

Syntax

```
config log device
  edit <device_string>
    set default-intf-type {dmz | wan | lan | none}
    set description <desc_str>
    set faz_owner <fortianalyzerid_str>
    set id <deviceid_str>
    set members-id <serialnum_str>
    set mode {HA | Standalone}
    set privileges <send-logs> <view-logs> <config-reports> <view-reports>
       <send-content> <view-content> <send-quarantine> <access-quarantine>
       <none>
    set psk <presharedkey_str>
    set secure {psk |none}
    set space <diskquota_int>
    set type {fgt | fmg | fml | syslog | all_forticlients}
    set when-full {overwrite | stop}
    config product-intf-type
      edit <interface_name>
        set intf-type {dmz | lan | none | wan}
      end
    config user-intf-types
      edit <interface_name>
        set intf-type {dmz | lan | none | wan}
      end
    end
```

Keywords and variables	Description	Default
`default-intf-type {dmz	wan	lan	none}`	Specify the interface type for the unlisted FortiGate interfaces. For example, on a FortiGate model, there are 8 interfaces marked as port 1 to 8. You have used the command “config product-intf-type” on page 43 to specify that port 1 is used as the LAN interface, port 2 is used as the WAN interface, and port 3 is used as the DMZ interface. Port 4 to 8 are unspecified/unlisted. Then you can use this command to specify how port 3 to 8 are be used by default. The interface information will be used to determine if the traffic is incoming or outgoing in the reports. For details, see “config product-intf-type” on page 43.	`none`
`description <desc_str>`	Enter a description of the device.	No default.
`faz_owner <fortianalyzerid_str>`	If the device is another FortiAnalyzer unit when this FortiAnalyzer unit is acting as a log aggregation server, enter the client FortiAnalyzer unit’s serial number.	No default.
`id <deviceid_str>`	If `secure` is `psk`, enter the device’s device ID (serial number).	No default.
`members-id <serialnum_str>`	If the device is an HA cluster, enter the device IDs (serial numbers) for each subordinate unit in the cluster.	No default.
`mode {HA	Standalone}`	Select whether the FortiGate unit is a standalone unit or a part of an HA cluster.	`Standalone`
`privileges <send-logs> <view-logs> <config-reports> <view-reports> <send-content> <view-content> <send-quarantine> <access-quarantine> <none>`	Set a list of privileges the device has to send and retrieve items from the FortiAnalyzer unit. For example, to allow a device to only send logs and quarantine, enter `set privileges send-logs send-quarantine`. Accessing logs, content logs and quarantined files is available on FortiGate units running firmware version 4.0 or later.	`access-quarantine config-reports send-content send-logs send-quarantine view-content view-logs view-reports` (all permissions granted)
`psk <presharedkey_str>`	If `secure` is `psk`, enter the preshared secret. The `psk` value must match the preshared secret (PSK) value configured on the device.	No default.

Keywords and variables	Description	Default
`secure {psk |none}`	Enable (`psk`) or disable (`none`) a secure tunnel for communications between the device and FortiAnalyzer unit. Once `secure` is set to `psk`, you must configure the IPSec VPN; the FortiAnalyzer unit cannot create the secure tunnel until it is configured. The secure tunnel must be configured on both ends of the tunnel: the FortiAnalyzer unit and the device. On a FortiAnalyzer, set `psk <presharedkey_str>` and `id <deviceid_str>`. On the device, enable the secure connection, then set the PSK and local ID (device name). Commands vary by device type. For specific instructions, see your device's CLI Reference.	`none`
`space <diskquota_int>`	Set the amount of disk space allocated for the device logs, content and quarantined files, in megabytes (MB).	Default varies by settings in `config log unregistered`.
`type {fgt | fmg | fml | syslog | all_forticlients}`	Select the type of device: • `fgt` for a FortiGate unit • `fmg` for a FortiManager unit • `fml` for a FortiMail unit • `syslog` for a Syslog server • `all_forticlients` for all FortiClients	Default varies by detected device type.
`when-full {overwrite | stop}`	Select what the FortiAnalyzer unit should do once the allocated disk space has been reached: overwrite older messages, or stop logging.	`overwrite`

Example

The following example adds a FortiGate unit named `FGT-60` with quarantine send and read and log send access.

```
config log device
  edit FGT-60
    set id FGT-60
    set privileges access-quarantine send-quarantine send-logs
    set type fgt
  end
```

The following example configures a secure tunnel for log and other data sent between the FortiAnalyzer unit and a FortiGate unit named `FGT-60`.

On the FortiAnalyzer unit:

```
config log device
  edit FGT-60
    set secure psk
    set psk SRE2IVN#seWNVd
    set id FGT60M2904400103
  end
```

On the FortiGate unit named `FGT-60`:

```
config system fortianalyzer
  set encrypt enable
  set psksecret SRE2IVN#seWNVd
  set localid FGT-60
end
```

config product-intf-type

After a FortiGate unit is added to the FortiAnalyzer unit, you need to assign each FortiGate network interface to a network interface class (None, LAN, WAN, or DMZ) based on your FortiGate network interface usage. Traffic between classes determines traffic flow directionality for reports.

- Using the config product-intf-type command, you can classify the FortiGate device's pre-defined network interfaces.
- Using the config user-intf-types command, you can classify the user-defined interfaces, such as the VLAN interface, loopback interface, IEEE 802.3ad aggregated interface, or redundant interface (for information about creating an interface, see the FortiGate Administration Guide).

Functionally classifying the device's network interfaces and VLAN subinterfaces as None, LAN, WAN or DMZ indirectly defines the directionality of traffic flowing between those network interfaces. For example, FortiAnalyzer units consider log messages of traffic flowing from a WAN class interface to a LAN or DMZ class interface to represent incoming traffic.

Some report types for FortiGate devices include traffic direction — inbound or outbound traffic flow. When the FortiAnalyzer unit generates reports involving traffic direction, the FortiAnalyzer unit compares values located in the source and destination interface fields of the log messages with your defined network interface classifications to determine the traffic directionality.

The table below illustrates the traffic directionality derived from each possible combination of source and destination interface class.

Table 10: Traffic directionality by class of the source and destination interface

Source interface class	Destination interface class	Traffic direction
None	All types	Unclassified
All types	None	Unclassified
WAN	LAN, DMZ	Incoming
WAN	WAN	External
LAN, DMZ	LAN, DMZ	Internal
LAN, DMZ	WAN	Outgoing

Syntax

```
config product-intf-types
  edit <interface_name>
    set intf-type {dmz | lan | none | wan}
  end
```

Keywords and variables	Description	Default
`<interface_name>`	Enter the name of the interface.	No default.
`intf-type {dmz	lan	none	wan}`	Select the logical type of the interface which will be used when interpreting log messages for report purposes.	No default.

Example

The following commands sets port 1 interface on the device `FGT-60` to be labeled as a DMZ-type interface.

```
config log device
  edit FGT-60
    config product-intf-types
      edit port1
        set intf-name port1
```

```
            set intf-type dmz
          end
      end
```

config user-intf-types

Use this subcommand to classify the user-defined FortiGate interfaces. For details, see “config user-intf-types” on page 44.

Syntax

```
config user-intf-types
  edit <interface_name>
    set intf-type {dmz | lan | none | wan}
  end
```

Keywords and variables	Description	Default
`<interface_name>`	Enter the name of the interface.	No default.
`intf-type {dmz	lan	none	wan}`	Select the logical type of the interface which will be used when interpreting log messages for report purposes.	No default.

Example

The following commands sets vlan1 interface on the device `FGT-60` to be labeled as a DMZ-type interface.

```
config log device
  edit FGT-60
    config user-intf-types
      edit port1
        set intf-name vlan1
        set intf-type dmz
      end
  end
```

History

3.0 MR1	Added `description`.
3.0 MR2	Added `Admin_Domains`, `faz_owner`, `members-id` and `mode`.
3.0 MR4	Removed `Admin_Domains`. It has been moved to `config Admin_Domain` and is available when ADOMs are enabled.
3.0 MR5	Added `vdom_num`.
3.0 MR7	Removed `vdom_num` keyword.

log device-group

Use this command to create groups to add and remove devices from this group. Use this command to group devices belonging to a department or section of the company to keep the devices together for easier monitoring and reporting.

Syntax

```
config log device-group
  edit <group_name>
```

```
    set devices <device_names>
    set type {fgt | fmg | fml | syslog}
  end
```

Keywords and variables	Description	Default
`<group_name>`	Enter the name of the device group.	No default.
`devices <device_names>`	Select the devices to add to the group. Use the Tab key to cycle through the available registered devices, or press the question mark (`?`) key to display devices that match your specified `type`. Separate multiple device names with a space.	No default.
`type {fgt	fmg	fml	syslog}`	Select the type of devices that can belong to this group. Device groups cannot contain devices of more than one type.	No default.

Example

The following example adds the devices `FGT-60` and `FGT-500` to the group `Finance`.

```
config log device-group
  edit Finance
    set type fgt
    set devices fgt-60 fgt-500
  end
```

log forwarding

Use this command to enable log forwarding and configure the Syslog server IP address. Messages meeting or exceeding only the minimum severity level will be forwarded.

Syntax

```
config log forwarding
  set forwarding {enabled | disabled}
  set forwarding_type {all_logs | permission_only}
  set min_level {emergency | alert | critical | error | warning | notification
      | information | debug}
  set remote_ip <ip_address>
end
```

Keywords and variables	Description	Default
`forwarding {enabled	disabled}`	Enable or disable log forwarding. If enabled, configure `remote_ip` to indicate the receiving Syslog server.	`disabled`
`forwarding_type {all_logs	permission_only}`	Select whether to forward all received log messages or to only forward authorized log messages.	`all_logs`
`remote_ip <ip_address>`	Enter the IP address of the receiving Syslog server.	No default.
`min_level {emergency	alert	critical	error	warning	notification	information	debug}`	Set the minimum severity threshold that a log message must meet or exceed to be forwarded to the `remote_ip`.	`information`

Example

The following configures the FortiAnalyzer unit to forward all log messages that meet or exceed alert level severity. The recipient Syslog server has the IP address 10.10.20.155.

```
config log forwarding
  set forwarding enabled
  set remote_ip 10.10.20.155
  set min_level alert
end
```

History

3.0 MR5	New command added.

log settings

Use this command and sub-command to configure the local log settings and log rolling settings for all log types, including Network Analyzer.

Syntax

```
config log settings
   set analyzer {enable | disable}
   set analyzer-interface [port1 | port2 | port3 | port4]
   set analyzer-quota <quota_int>
   set analyzer-quota-full {overwrite | stop}
   set analyzer-settings {device | custom}
   set FCT-custom-field1 <field_name>
   set FCT-custom-field2 <field_name>
   set FCT-custom-field3 <field_name>
   set FCT-custom-field4 <field_name>
   set FCT-custom-field5 <field_name>
   set FGT-custom-field1 <field_name>
   set FGT-custom-field2 <field_name>
   set FGT-custom-field3 <field_name>
   set FGT-custom-field4 <field_name>
   set FGT-custom-field5 <field_name>
   set local {enable | disable}
   set local-filter {config | ipmac | ipsec | login | system}
   set local-level {emergency | alert | critical | error | warning |
      notification | information | debug}
   set local-quota <integer>
   set local-quota-full {overwrite | stop}
   set local-settings {device | custom}
   set mms-gui {enable | disable}
   set syslog {enable | disable}
   set syslog-csv {enable | disable}
   set syslog-filter {config | ipsec | login | system | none}
   set sylog-ip <ip_address>
   set syslog-level {emergency | alert | critical | error | warning |
      notification | information | debug}
   set syslog-port <port_number>
     config rolling-analyzer
```

```
    set days {mon | tue | wed | thu | fri | sat | sun}
    set del-files {enable | disable}
    set directory <dir_str>
    set filesize <size_int>
    set gzip-format {enable | disable}
    set hour <integer>
    set ip <ip_address>
    set min <integer>
    set password <password_str>
    set server_type {FTP | SCP | SFTP}
    set upload {enable | disable}
    set upload-hour [0-24]
    set upload-trigger {on-roll | on-schedule}
    set username <username_str>
    set when {daily | weekly | none}
  end
    config rolling-local
      set days {mon | tue | wed | thu | fri | sat | sun}
      set del_files {enable | disable}
      set directory <dir_str>
      set filesize <size_int>
      set gzip_format {enable | disable}
      set hour <integer>
      set min <integer>
      set ip <ip_address>
      set password <password_str>
      set upload {enable | disable}
      set upload-hour [0-24]
      set upload-trigger {on-roll | on-schedule}
      set username <username_str>
      set server_type {FTP | SCP | SFTP}
      set when {daily | weekly | none}
    end
      config rolling-regular
        set days {mon | tue | wed | thu | fri | sat | sun}
        set del_files {enable | disable
        set directory <dir_str>
        set filesize <size_int>
        set gzip_format {enable | disable}
        set hour <integer>
        set ip <ip_address>
        set min <integer>
        set password <password_str>
        set upload {enable | disable}
        set upload-hour [0-24]
        set upload-trigger {on-roll | on-schedule}
        set username <username_str>
        set server_type {FTP | SCP | SFTP}
        set when {daily | weekly | none}
    end
end
```

Keywords and variables	Description	Default
`analyzer {enable | disable}`	Enter to enable network FortiAnalyzer.	`disable`
`analyzer-interface [port1 | port2 | port3 | port4]`	Enter the network interface that will be recording traffic from.	No default
`analyzer-quota <quota_int>`	Enter the amount of disk space to allocate to logging network traffic. A value of 0 (zero) is unlimited.	`1000`
`analyzer-quota-full {overwrite | stop}`	Set what the FortiAnalyzer unit does when the allocated traffic log space is full. Select overwrite to `overwrite` older log data, select `stop` to stop logging until the administrator can backup the logs and clear the disk space.	`overwrite`
`analyzer-settings {device | custom}`	Enter `custom` to use the custom settings for rolling and uploading Network Analyzer logs. Enter `device` to re-use log settings for rolling and uploading Network Analyzer logs.	`device`
`FCT-custom-field1 <field_name>`	Enter the custom field that was entered on the FortiClient Endpoint Security. This command enables the FortiClient custom field to be properly indexed by the FortiAnalyzer unit. You can enter up to five FortiClient custom fields.	No default
`FCT-custom-field2 <field_name>`	Enter the custom field that was entered on the FortiClient Endpoint Security. This command enables the FortiClient custom field to be properly indexed by the FortiAnalyzer unit.	No default
`FCT-custom-field3 <field_name>`	Enter the custom field that was entered on the FortiClient Endpoint Security. This command enables the FortiClient custom field to be properly indexed by the FortiAnalyzer unit.	No default
`FCT-custom-field4 <field_name>`	Enter the custom field that was entered on the FortiClient Endpoint Security. This command enables the FortiClient custom field to be properly indexed by the FortiAnalyzer unit.	No default
`FCT-custom-field5 <field_name>`	Enter the custom field that was entered on the FortiClient Endpoint Security. This command enables the FortiClient custom field to be properly indexed by the FortiAnalyzer unit.	No default
`FGT-custom-field1 <field_name>`	Enter the custom field that was entered on the FortiGate unit. This command enables the FortiGate custom field to be properly indexed by the FortiAnalyzer unit. You can enter up to five FortiGate custom fields.	No default
`FGT-custom-field2 <field_name>`	Enter the custom field that was entered on the FortiGate unit. This command enables the FortiGate custom field to be properly indexed by the FortiAnalyzer unit.	No default
`FGT-custom-field3 <field_name>`	Enter the custom field that was entered on the FortiGate unit. This command enables the FortiGate custom field to be properly indexed by the FortiAnalyzer unit.	No default
`FGT-custom-field4 <field_name>`	Enter the custom field that was entered on the FortiGate unit. This command enables the FortiGate custom field to be properly indexed by the FortiAnalyzer unit.	No default
`FGT-custom-field5 <field_name>`	Enter the custom field that was entered on the FortiGate unit. This command enables the FortiGate custom field to be properly indexed by the FortiAnalyzer unit.	No default
`local {enable | disable}`	Enter to enable logging to the local hard disk.	`disable`
`local-filter {config | ipmac | ipsec | login | system}`	Select the events the FortiAnalyzer logs to the hard disk. Use this keyword in conjunction with `local_loglevel`.	`config ipsec login system`
`local-level {emergency | alert | critical | error | warning | notification | information | debug}`	Enter the local log severity level.	`information`

Keywords and variables	Description	Default
`local-quota <integer>`	Enter the amount of disk space to allocate for local logs. A value of 0 (zero) is unlimited.	0
`local-quota-full {overwrite | stop}`	Set what the FortiAnalyzer unit does when the allocated local log space is full. Select overwrite to `overwrite` older log data, select `stop` to stop logging until the administrator can backup the logs and clear the disk space.	overwrite
`local-settings {device | custom}`	Enter to roll and upload local logs. Enter custom to use custom settings.	device
`mms-gui {enable | disable}`	Enter to show the archived MMS logs on the web-based manager. This applies when only there are MMS logs stored on the FortiAnalyzer unit. MMS logs are recorded when a FortiGate unit is running FortiOS Carrier.	disable
`syslog {enable | disable}`	Enter to enable logging to a Syslog server.	disable
`syslog-csv {enable | disable}`	Enter to enable the log format CSV for logs.	disable
`syslog-filter {config | ipsec | login | system | none}`	Enter to include logs that are related to configuration changes (config), IPSec connections (ipsec), administrative logins and logouts (login), and system activity (system). If you enter none, no logs will be included.	none
`sylog-ip <ip_address>`	Enter the IP address of the Syslog server.	0.0.0.0
`syslog-level {emergency | alert | critical | error | warning | notification | information | debug}`	Enter the syslog log severity level.	emergency
`syslog-port <port_number>`	Enter the Syslog server's port number, if different from the default port 514.	514

Example

The following commands enable local logging on the FortiAnalyzer unit.

```
config log settings
    set local enable
    set local-settings custom
    set local-quota 100
    set local-quota-full overwrite
    set local-level error
    set local-filter login system config
  end
```

History

3.0 MR4	Removed `content_reuse_logs` and config rolling content commands. These settings are rolled into `config rolling-analyzer.`
3.0 MR5	Changed effects of `enable_analyzer` to also enable Network Analyzer's appears on the web-based manager.

3.0 MR7	Removed `show_mms_option` and added `show_mms_archive` keyword. Added the following keywords: • `custom-field1` • `custom-field2` • `custom-field3` • `custom-field4` • `custom-field5`
4.0 MR2	Removed `analyzer-gui` and added: • `FCT-custom-field1` • `FCT-custom-field2` • `FCT-custom-field3` • `FCT-custom-field4` • `FCT-custom-field5` • `FGT-custom-field1` • `FGT-custom-field2` • `FGT-custom-field3` • `FGT-custom-field4` • `FGT-custom-field5`

config rolling-analyzer

Use this sub-command to configure the log rolling of the Network Analyzer logs. You must first set the `analyzer-settings` to `custom` so that you can view the sub-commands. If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

Syntax

```
config rolling-analyzer
   set days {mon | tue | wed | thu | fri | sat | sun}
   set del-files {enable | disable}
   set directory <dir_str>
   set filesize <size_int>
   set gzip-format {enable | disable}
   set hour <integer>
   set ip <ip_address>
   set min <integer>
   set server_type {FTP | SCP | SFTP}
   set upload {enable | disable}
   set upload-hour [0-24]
   set upload-trigger {on-roll | on-schedule}
   set username <username_str>
   set password <password_str>
   set when {daily | weekly | none}
end
```

Keywords and variables	Description	Default
`days {mon	tue	wed	thu	fri	sat	sun}`	Enter day of the week when the FortiAnalyzer rolls the traffic analyzer logs. This variable becomes available when setting the `when` variable to `weekly`.	No default.
`del-files {enable	disable}`	Enable to delete the log files from the FortiAnalyzer hard disk one uploading is complete.	`disable`
`directory <dir_str>`	Select a directory on the upload server where the FortiAnalyzer unit stores the uploaded logs.	No default.

Keywords and variables	Description	Default
`filesize <size_int>`	The maximum size of the current log file that the FortiAnalyzer unit saves to the disk. When the log file reaches the specified maximum size, the FortiAnalyzer unit saves the current log file and starts a new active log file. When a log file reaches its maximum size, the FortiAnalyzer unit saves the log files with an incremental number, and starts a new log file with the same name.	`100`
`gzip-format {enable | disable}`	Enable to compress the log files using the gzip format.	`disable`
`hour <integer>`	Enter the hour of the day when the when the FortiAnalyzer rolls the traffic analyzer logs.	`0`
`ip <ip_address>`	Enter the upload server ip address.	`0.0.0.0`
`min <integer>`	Enter the minute when the FortiAnalyzer rolls the traffic analyzer logs.	`0`
`server_type {FTP | SCP | SFTP}`	Select the type of upload server.	`FTP`
`upload {enable | disable}`	Enable the FortiAnalyzer unit to upload the rolled log file to an FTP site. When selecting yes, use the `set host_ip` and `set port_integer` to define the FTP location.	`disable`
`upload-hour [0-24]`	Enter the hour that you want to upload the log files. The default is zero. Enter the number, without minutes, in the 24-hour format (0-24).	`0`
`upload-trigger {on-roll | on-schedule}`	Enter what type of trigger will upload log files. The trigger `on-roll` will upload log files whenever they roll. The trigger `on-schedule` will upload log files on a scheduled basis.	`on-roll`
`username <username_str>`	Enter the user name for the upload server.	No default
`password <password_str>`	Enter the password for the upload server user name.	No default.
`when {daily | weekly | none}`	Set the frequency of when the FortiAnalyzer unit saves the current log file and starts a new active log file. Select this option if you want to start new log files even if the maximum log file size has not been reached. For example, you want to roll a daily log on a FortiAnalyzer unit that does not see a lot of activity.	`none`

Example

The following sub-commands enables log rolling when log files are 100 MB.

```
config log settings
  config rolling-analyzer
    set filesize 100
  end
end
```

History

3.0 MR1 Added uploading options for scheduling uploading times and locations.

config rolling-local

Use this sub-command to configure the log rolling of the FortiAnalyzer unit local logs. If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

This sub-command becomes available only when `local-settings` is set to `custom`.

Syntax

```
config rolling-local
  set days {mon | tue | wed | thu | fri | sat | sun}
  set del_files {enable | disable}
  set directory <dir_str>
  set filesize <size_int>
  set gzip_format {enable | disable}
  set hour <integer>
  set min <integer>
  set ip <ip_address>
  set password <password_str>
  set upload {enable | disable}
  set upload-hour [0-24]
  set upload-trigger {on-roll | on-schedule}
  set username <username_str>
  set server_type {FTP | SCP | SFTP}
  set when {daily | weekly | none}
end
```

Keywords and variables	Description	Default
`days {mon | tue | wed | thu | fri | sat | sun}`	Enter day of the week when the FortiAnalyzer rolls the current logs. This variable becomes available when setting the `when` variable to `weekly`.	No default.
`del_files {enable | disable}`	Enable to delete the log files from the FortiAnalyzer hard disk one uploading is complete.	`disable`
`directory <dir_str>`	Select a directory on the upload server where the FortiAnalyzer unit stores the uploaded logs.	No default
`filesize <size_int>`	The maximum size of the current log file that the FortiAnalyzer unit saves to the disk. When the log file reaches the specified maximum size, the FortiAnalyzer unit saves the current log file and starts a new active log file. When a log file reaches its maximum size, the FortiAnalyzer unit saves the log files with an incremental number, and starts a new log file with the same name.	`100`
`gzip_format {enable | disable}`	Enable to compress the log files using the gzip format.	`disable`
`hour <integer>`	Enter the hour of the day when the when the FortiAnalyzer rolls the current logs.	`0`
`min <integer>`	Enter the minute when the FortiAnalyzer rolls the traffic analyzer logs.	`0`
`ip <ip_address>`	Enter the upload server IP address.	`0.0.0.0`
`password <password_str>`	Enter the password for the upload server user name	No default
`upload {enable | disable}`	Enable the FortiAnalyzer unit to upload the rolled log file to an FTP site. When selecting yes, use the `set host_ip` and `set host_port` to define the FTP location.	`no`
`upload-hour [0-24]`	Enter the hour that you want to upload the log files. The default is zero. Enter the number, without minutes, in the 24-hour format (0-24).	`0`
`upload-trigger {on-roll | on-schedule}`	Enter what type of trigger will upload log files. The trigger `on-roll` will upload log files whenever they roll. The trigger `on-schedule` will upload log files on a scheduled basis.	`on-roll`
`username <username_str>`	Enter the user name for the upload server.	No default

Keywords and variables	Description	Default
`server_type {FTP	SCP	SFTP}`	Select the type of upload server	`FTP`
`when {daily	weekly	none}`	Set the frequency of when the FortiAnalyzer unit saves the current local log file and starts a new active log file. Select this option if you want to start new log files even if the maximum log file size has not been reached. For example, you want to roll a daily log on a FortiAnalyzer unit that does not see a lot of activity.	`none`

Example

The following sub-commands enables log rolling when log files are 100 MB.

```
config log settings
  config rolling-local
    set filesize 100
  end
end
```

History

3.0 MR1	Added uploading options for scheduling uploading times and locations.

config rolling-regular

Use this sub-command to configure the log rolling of the device logs. If the log upload fails, such as when the FTP server is unavailable, the logs are uploaded during the next scheduled upload.

Syntax

```
config rolling-regular
   set days {mon | tue | wed | thu | fri | sat | sun}
   set del_files {enable | disable
   set directory <dir_str>
   set filesize <size_int>
   set gzip_format {enable | disable}
   set hour <integer>
   set ip <ip_address>
   set min <integer>
   set password <password_str>
   set upload {enable | disable}
   set upload {enable | disable}
   set upload-hour [0-24]
   set upload-trigger {on-roll | on-schedule}
   set username <username_str>
   set server_type {FTP | SCP | SFTP}
   set when {daily | weekly | none}
end
```

Keywords and variables	Description	Default
`days {mon | tue | wed | thu | fri | sat | sun}`	Enter day of the week when the FortiAnalyzer rolls the current logs. This variable becomes available when setting the `when` variable to `weekly`.	No default.
`del_files {enable | disable`	Enable to delete the log files from the FortiAnalyzer hard disk one uploading is complete.	`disable`
`directory <dir_str>`	Select a directory on the upload server where the FortiAnalyzer unit stores the uploaded logs.	No default.
`filesize <size_int>`	The maximum size of the current log file that the FortiAnalyzer unit saves to the disk. When the log file reaches the specified maximum size, the FortiAnalyzer unit saves the current log file and starts a new active log file. When a log file reaches its maximum size, the FortiAnalyzer unit saves the log files with an incremental number, and starts a new log file with the same name. A value of 0 (zero) is unlimited.	`0`
`gzip_format {enable | disable}`	Enable to compress the log files using the gzip format.	`disable`
`hour <integer>`	Enter the hour of the day when the when the FortiAnalyzer rolls the current logs.	`0`
`ip <ip_address>`	Enter the upload server ip address.	`0.0.0.0`
`min <integer>`	Enter the minute when the FortiAnalyzer rolls the current logs.	`0`
`password <password_str>`	Enter the password for the upload server user name.	No default.
`upload {enable | disable}`	Enable the FortiAnalyzer unit to upload the rolled log file to an FTP site. When selecting yes, use the `set host_ip` and `set host_port` to define the FTP location.	`no`
`upload-hour [0-24]`	Enter the hour that you want to upload the log files. The default is zero. Enter the number, without minutes, in the 24-hour format (0-24).	`0`
`upload-trigger {on-roll | on-schedule}`	Enter what type of trigger will upload log files. The trigger `on-roll` will upload log files whenever they roll. The trigger `on-schedule` will upload log files on a scheduled basis.	`on-roll`
`username <username_str>`	Enter the user name for the upload server.	No default
`server_type {FTP | SCP | SFTP}`	Select the type of upload server.	`FTP`
`when {daily | weekly | none}`	Set the frequency of when the FortiAnalyzer unit saves the current log file and starts a new active log file. Select this option if you want to start new log files even if the maximum log file size has not been reached. For example, you want to roll a daily log on a FortiAnalyzer unit that does not see a lot of activity.	`none`

Example

The following sub-commands enables log rolling when log files are 100 MB.

```
config log settings
  config rolling-regular
    set filesize 100
  end
end
```

History

3.0 MR1	Added uploading options for scheduling uploading times and locations.

log unregistered

Use this command to configure how the FortiAnalyzer unit handles unregistered devices as they connect to the FortiAnalyzer unit.

As devices are configured to send log packets to the FortiAnalyzer unit, you can configure how the FortiAnalyzer unit handles the connection requests until you can verify they should be accepted. You can define what the FortiAnalyzer unit does when it receives a request for a connection from a device.

Syntax

```
config log unregistered
   set blocked-devices <serial_number>
   set handling {drop-logs-only | drop-all | save-logs}
   set known-handling {save-logs | drop-all | drop-logs-only}
   set known-quota <knownquota_int>
   set quota <quota_int>
end
```

Keywords and variables	Description	Default
`blocked-devices <serial_number>`	Enter the devices the FortiAnalyzer unit blocks from submitting log data.	No default.
`handling {drop-logs-only | drop-all | save-logs}`	Select how the FortiAnalyzer handles a connection request from an unknown device. Select from the following: • `drop-all` - All incoming device requests are not accepted and the FortiAnalyzer will not add them to the unregistered devices list. • `drop-logs-only` - Add the device to the unregistered devices list for future configuration and addition to the FortiAnalyzer unit, but do not save the incoming log packets to the hard disk. • `save-logs` - Add the device to the unregistered devices list for future configuration and addition to the FortiAnalyzer unit, and save the log packets to the hard disk, but only to a defined amount of disk space. Set the disk space using the keyword `quota`.	`drop-logs-only`
`known-handling {save-logs | drop-all | drop-logs-only}`	Select how the FortiAnalyzer handles a connection request from an known device. Select from the following: • `drop-all` - All incoming device requests are not accepted and the FortiAnalyzer will not add them to the unregistered devices list. • `drop-logs-only` - Add the device to the unregistered devices list for future configuration and addition to the FortiAnalyzer unit, but do not save the incoming log packets to the hard disk. • `save-logs` - Add the device to the unregistered devices list for future configuration and addition to the FortiAnalyzer unit, and save the log packets to the hard disk, but only to a defined amount of disk space. Set the disk space using the keyword `known_quota`.	`save-logs`
`known-quota <knownquota_int>`	Enter the amount of disk space to allocate to collecting log data for a known device until the device is registered.	`100`
`quota <quota_int>`	Enter the amount of disk space to allocate to collecting log data for an unknown device until the device is registered.	`20`

Example

The following commands sets the handling of unknown devices to allow the connection and saving the logs up to 50 MB.

```
config log unregistered
  set handling save-logs
  set quota 30
end
```

nas group

Use this command to add a group for users and add or remove members from the group. When adding groups, you must first add members using the `config nas user` command. For more information about NAS users, see "nas user" on page 58.

Syntax

```
config nas group
   edit <group_str>
      set gid <groupid_int>
      set members <usernames_str>
   end
```

Keywords and variables	Description	Default
`<group_str>`	Enter the name for the group.	No default.
`gid <groupid_int>`	If the group uses NFS shares, enter a group ID.	No default.
`members <usernames_str>`	Enter a list of the users to include in the group.	No default.

Example

The following commands add `user_1` and `user_2` to the group `local_group`.

```
config nas group
     edit local_group
         set members user_1 user_2
   end
```

nas nfs

Use this command to configure NFS network share file permissions.

Syntax

```
config nas nfs
   <interface_name>
      set ro <username_str>
      set rw <useruname_str>
   end
```

Keywords and variables	Description	Default
`edit <path_str>`	Enter the name of the local path which is an NFS share.	No default.
`ro <username_str>`	Enter a list of users with read-only access to the directory.	No default.
`rw <useruname_str>`	Enter a list of users with read and write access to the directory.	No default.

Example

You could add the user `User_1` to the local path `/reports` with read-only access.

```
config nas nfs
  edit reports
    set ro User_1
 end
```

nas protocol

Use this command to enable either NFS or Windows file shares on the FortiAnalyzer unit.

Syntax

```
config nas protocol
   set nfs{enabled | disabled}
   set share {enabled | disabled}
   set workgroup <workgroupname_str>
 end
```

Keywords and variables	Description	Default
`nfs{enabled | disabled}`	Enable or disable Network File Sharing (NFS) on the FortiAnalyzer.	`disabled`
`share {enabled | disabled}`	Enable or disable Windows networking on the FortiAnalyzer. When enabled, also set the `workgroup`.	`disabled`
`workgroup <workgroupname_str>`	If `share` in `enabled`, enter the name of the Windows workgroup.	No default.

Example

You could enable Windows networking with a workgroup named `Co_Reports`.

```
config nas protocol
   set share enabled
   set workgroup Co_Reports
 end
```

nas share

Use this command to configure Windows network share file permissions and paths.

Note: You can only share folders below the `/Storage` folder.

Syntax

```
config nas share
 edit <share_str>
   set path <path_str>
   set ro <name_str>
   set rw <name_str>
 end
```

Keywords and variables	Description	Default
`edit <share_str>`	Enter the name of the networking share.	No default.
`path <path_str>`	Enter the name of the local networking path.	No default.
`ro <name_str>`	Enter a list of users with read-only access to the directory.	No default.
`rw <name_str>`	Enter a list of users with read and write access to the directory.	No default.

Example

The following example adds the user `User_1` to the local path `reports` with read-only access.

```
config nas share
    edit reports
        set path reports
        set ro User_1
  end
```

nas user

Use this command to add and maintain users who can access the FortiAnalyzer hard disk.

Syntax

```
config nas user
  edit <name_str>
     set display <description_str>
     set password <password_str>
     set uid <userid_int>
  end
```

Keywords and variables	Description	Default
`edit <name_str>`	Enter the name of the user.	No default.
`display <description_str>`	Enter a description for the user.	No default.
`password <password_str>`	Enter the user’s password.	No default.
`uid <userid_int>`	Enter a user ID. Use this keyword only if you are using the NFS protocol. The NFS protocol uses the UID to determine the permissions on files and folders.	No default.

Example

The following example adds the user `User_1` with a displayed description of `A NAS user.`, a password of `passw0rd` and a user id of `15`.

```
config nas user
    edit User_1
        set display “A NAS user.”
        set password passw0rd
        set uid 15
  end
```

report chart

Use this command to configure a customized chart or edit an existing chart for your reports. Before using this command, you must first configure a dataset using the `dataset` command because you need a dataset when configuring a chart. All configured charts appear in the Custom Charts list when adding charts to a report layout.

Syntax

```
config report chart
  edit <chart_name>
    set comment <string>
    set dataset <dataset_name>
    set graph-type {bar | pie}
    set title <chart_name>
    set type {graph | table | table-graph}
  end
```

Keywords and variables	Description	Default
`<chart_name>`	Enter a name for the chart or enter an existing name to edit.	No default
`comment <string>`	Enter a comment or description for the chart. The comment or description should contain underscores (_) between each word or quotes, for example, “Report_chart_June_2009”.	No default
`dataset <dataset_name>`	Enter the dataset that you want to use for the chart.	No default
`graph-type {bar | pie}`	Enter the type of graph that will be used in the chart.	No default
`title <chart_name>`	Enter a name for the chart’s title. When choosing custom charts in *Report* > *Config* > *Layout*, this name appears in the Custom Charts list.	No default
`type {graph | table | table-graph}`	Enter the type of format the information will appear in, either a table, graph, or both.	No default

Example

The following configures a new customized chart for a report layout.

```
config report chart
  edit chart_1
    set comment “Report_for_June_2009”
    set dataset data_june09
    set graph-type pie
    set title “Top websites for .125 users”
    set type table-graph
  end
```

History

4.0 MR1	New.

report dataset

Use this command to configure datasets that will be used when configuring customized charts using the `chart` command. A dataset must be configure first, before configuring a chart, because the chart must contain a dataset.

Before configuring datasets, you need to first go through and find which log type you want to have in your customized dataset. You need to know the log type because you can only have one log type per dataset. When configuring the dataset with the chosen log type, you also need to know which log fields you want to filter for that log type. For example, you choose `app-crtl` and then choose the log fields `app` and `app_type`.

Datasets must be configured in the order the variables appear in the following Syntax. You must also enter the type of log (`log-type`) before enter the filtering information (`filter <field>`). Each dataset contains only one log type.

Syntax

```
config report dataset
  edit <dataset_name>
    set filter <field>
    set log-type {app-crtl | attack | content | dlp | emailfilter | event |
       history | im | none | traffic | virus | voip | webfilter}
    config output
      edit <output_number>
        set group-priority {primary-key | secondary-key}
        set sort-by {by-key-asc | by-key-dsc | by-value}
        set top <top_number>
        set type {derived-field| field | function}
        set value {derived-field name | field name | function name}
      next
    config field
      edit <field_number>
        set display-name <name_field>
        set output <output_id>
      next
end
```

Keywords and variables	Description	Default

`filter <field>`	Enter a field to filter the information. The available operators are:
	`==` OR `!=`
	The available combinations, if using two fields, must include `&&` and be used in the following way:
	`subtype==infected&&service=imap`
	When you are including spaces, use quotes around the words. For example, `user==“user 1”`. If you are stating a set of possible values, use curly braces as in the following example:
	`user=={user1 “super admin” user_1}`
	The available fields appear only when you enter ? at the end of the line. They are also specific to the log-type that you chose.
	Note: The list of fields depends on the chosen log type. The list includes only indexed log fields.
		No default

`log-type {app-crtl | attack | content | dlp | emailfilter | event | history | im | none | traffic | virus | voip | webfilter}`	Enter a type of log you want for the dataset. You can only choose one log type for each dataset. Multiple log types are not supported. **Note:** You must enter a log type before entering the filter information.	No default

config output

Use this command to configure the outputs for the dataset. This must be configured before configuring the fields. When configuring the output, you should consider the following query combinations:

- one field and one function
- one derived field and one function
- two fields and one function
- one derived field, one field and one function

The output requires one of the above query combinations, such as one field and one function.

Syntax

```
config output
  edit <output_number>
    set group-priority {primary-key | secondary-key}
    set sort-by {by-key-asc | by-key-dsc | by-value}
    set top <top_number>
    set type {derived-field| field | function}
    set value {derived-field name | field name | function name}
  next
end
```

Keywords and variables	Description	Default
`<output_number>`	Enter a sequential number for the output. For example, enter 1 for the first output.	No default
`group-priority {primary-key | secondary-key}`	Enter the number that indicates which output should be taken with higher priority when sorting the results. This number is either 1 (primary-key) or 2 (secondary-key). For example, if the outputs are src (group_priority 1), dst (group_priority 2), and add(sent,rcvd), then the sorting is for the total traffic which is the third column of top sources (which is the first column) by top destinations (which is the second column).	No default
`sort-by {by-key-asc | by-key-dsc | by-value}`	Enter to sort by ascending, descending or value. This appears after entering a group-priority for the first output.	No default

Keywords and variables	Description	Default
`top <top_number>`	Enter the top number of entries.	No default
`type {derived-field| field | function}`	Enter the type of query you want for the dataset. • **derived-field** – A value that is derived from one or more log message fields which is used for grouping the query results. • **field** – An unprocessed log message field which is used for grouping the query's results. • **function** – A computation done on all the logs that corresponds to the unique values of the fields or derived fields.	No default
`value {derived-field name | field name | function name}`	The derived-field or function name that appears in the list. You must enter `?` after entering `set value`, so that you can choose a value from the list.	No default

config field

Use this command to configure the fields for the dataset.

Syntax

```
config field
  edit <field_number>
    set display-name <name_field>
    set output <output_id>
  next
end
```

Keywords and variables	Description	Default
`<field_number>`	Enter a sequential number for the field. For example, enter 1 for the first field.	No default
`display-name <name_field>`	Enter a name for the field that will appear on the chart.	No default
`output <output_id>`	Enter the ID number of the output you want associated with the field.	No default

Example

The following configures a new dataset.

```
config report dataset
  edit dataset_1
    set display-name ds1
    set output 1
  end
```

History

4.0 MR1	New.

report filter

Use this command to configure a filter template to be used with a report schedule.

Syntax

```
config report filter
  edit <filter_name>
```

```
        set description <string>
        set filter-dst <destination_ip_address>
        set filter-email-direction <direction_name>
        set filter-email-domain <domain_name>
        set filter-email-from <email_address>
        set filter-email-to <email_address>
        set filter-generic <generic_text>
        set filter-interface <network_interface>
        set filter-iwday {sun | mon | tue | wed | thu | fri | sat}
        set filter-logic {all | any}
        set filter-policyid <firewallpolicy_number>
        set filter-priority {emergency | alert | cirtical | error | warning |
           notification | information | debug}
        set filter-service <service_name>
        set filter-src <source_ip_address>
        set filter-web-category [<number_1> | <number_2> | <number_3>…]
      end
```

Keywords and variables	Description	Default
`edit <filter_name>`	Enter a name for the filter template.	No default
`description <string>`	Enter a description to describe the filter template. This is optional.	No default
`filter-dst <destination_ip_address>`	Enter the destination IP address or multiple destination IP addresses.	No default
`filter-email-direction <direction_name>`	Enter to filter the direction of where email messages are coming from, either out or unknown.	No default
`filter-email-domain <domain_name>`	Enter to filter email messages by domain name for either the receiver of the email message or sender of the email message. This is used only for FortiMail logs.	No default
`filter-email-from <email_address>`	Enter to filter the email messages from the specified email sender address.	No default
`filter-email-to <email_address>`	Enter to filter the email messages to the specified email recipient address.	No default
`filter-generic <generic_text>`	Enter both the keyword and value number for the generic filter list. Do not include a space between the keyword and value number.	No default
`filter-interface <network_interface>`	Enter the network interface or multiple network interfaces to include matching logs.	No default
`filter-iwday {sun | mon | tue | wed | thu | fri | sat}`	Enter a day of the week for filtering. You can enter multiple days, separated by a space.	No default
`filter-logic {all | any}`	Enter the filter logic for the filter template. If you select `all`, only logs in the report that match all the filter criteria will be included. If you select `any`, only logs in the report that match any of the filter criteria.	No default
`filter-policyid <firewallpolicy_number>`	Enter the FortiGate firewall policy ID numbers to include matching logs.	No default
`filter-priority {emergency | alert | cirtical | error | warning | notification | information | debug}`	Enter the priority level for the filter template. You can enter multiple priority levels, by separating each with a space.	No default
`filter-service <service_name>`	Enter the service to include matching logs.	No default

Keywords and variables	Description	Default
`filter-src <source_ip_address>`	Enter the source IP address or multiple source IP addresses.	No default
`filter-web-category [<number_1> | <number_2> | <number_3>…]`	Enter a web category. Numbers (1-90) represent each web category including sub-web categories. You must separate each number with a comma. For example, if you enter 1,2, the first web category Potentially Liable is selected, as well as the first two sub-web categories within Potentially Liable, Drug Abuse and Occult. Fortinet recommends reviewing the web-based manager to verify that the applicable web-categories are selected.	No default

Example

The following configures a new filter template for a report schedule.

```
config report filter
  edit filter_1
    set description for_branch_office_use_only
    set filter-logic all
    set filter-priority emergency critical warning
    set filter-iwday mon wed fri
    set filter-interface port1,port2,port3
    set filter-web-category 1,2,3,11,7,8.5
    set filter-generic june1
  end
```

History

3.0 MR7	New.

report language

Use this command to enter a description for a language that will be included in the report. You need to import the language file before editing the file. Use the command “execute import-lang” on page 130 to import the language.

Syntax

```
config report language
  edit <language_name>
    set description
  end
```

Keywords and variables	Description	Default
`edit <language_name>`	Enter the language you want to add a description to. The languages that are available are English, Simplified Chinese, Traditional Chinese, Japanese, and Spanish.	`English`
`description`	Enter a description for the language you selected. This limit is 127 lines.	The name of the language is the default description

History

3.0 MR7	New.

report layout

Use this command to configure the layout for the report to be generated. The report layout includes charts, devices, and if applicable, filter templates.

Syntax

```
config report layout
  edit <layout_name>
    set company <name_company>
    set description <string>
    set dev-type {FortiGate | FortiClient | FortiMail}
    set footer-options {report-title | custom}
    set header-comment <comment_str>
    set header-logo-file <directory_path>
    set include-no-data {enable | disable}
    set include-summary {enable | disable}
    set obfuscate-user {enable | disable}
    set table-of-content {enable | disable}
    set title <title_name>
    set title-logo-file <directory_path>
    config object
      edit <obj_id>
        set category [FortiGate{fgt-intrusion | fgt-antivirus |fgt-webfilter |
            fgt-mailfilter | fgt-im | fgt-content | fgt-network | fgt-web |
            fgt-mail | fgt-ftp | fgt-terminal | fgt-vpn | fgt-event | fgt-p2p |
            fgt-voip}] [FortiClient {fct-antivirus | fct-network | fct-
            webfilter | fct-mailfilter}] [FortiMail {fml-highlevel | fml-mail |
            fml-spam | fml-virus}
        set description <comment_str>
        set devices [<device_1> | <device_2> | <device_3> ...]
        set device-mode [variable | specify]
        set filter <filter_name>
        set filter-mode [variable | specify]
        set group <group_name>
        set group-mode [variable | specify]
        set ldap-case-sensitive {enable | disable}
        set ldap-query [enable | disable]
        set ldap-server <server_name>
        set name [<chart_name1> | <chart_name2> | <chart_name3>...]
        set order <integer>
        set period-mode [variable | specify]
        set period-opt [dev | faz]
        set period-type [today | yesterday | last-n-hours | this-week | last-
            7-days | last-n-days | last-2-weeks | last-14-days | this-month |
            last-30-days | last-n-weeks | this-quarter | last-quarter | this-
            year | other]
        set resolve-host [enable | disable]
        set resolve-service [enable | disable]
        set source-id [user | ip | both]
        set style [pie | bar | line]
        set table-graph [all | table | graph]
        set table-top2 <integer>
        set topn <integer>
        set type [chart | section | text]
        set user <user_name>
        set user-mode [variable | specify]
        set vd <virtual_domain_name>
        set vd-mode [variable | specify]
    end
```

Keywords and variables	Description	Default
`edit <layout_name>`	Enter a name for the report layout.	No default
`company <name_company>`	Enter the name of the company or organization. This is optional.	No default
`description <string>`	Enter a description for the report layout. This is optional.	No default
`dev-type {FortiGate | FortiClient | FortiMail}`	Enter the type of device the log information will come from.	No default
`footer-options {report-title | custom}`	Enter either report-title, to include the title of the report for the footer, or customize the footer.	No default
`header-comment <comment_str>`	Enter what should be in the header of the report.	No default
`header-logo-file <directory_path>`	Enter the path and file name to small logo to use in the header. The logo will be uploaded to the FortiAnalyzer hard disk. When adding a logo to the report, consider the following to ensure you select the correct logo format for the report. If you select a log that is not supported for a report format, the logo will not appear in the report. • PDF reports – JPG and PNG • RTF reports – JPG, PNG, GIF, and WMF • HTML reports – all bitmap formats	No default
`include-no-data {enable | disable}`	Enable or disable to include or hide empty reports because there is no matching log data.	`disable`
`include-summary {enable | disable}`	Enable or disable to include a summary of the report information.	`enable`
`obfuscate-user {enable | disable}`	Enter enable or disable for user.	`disable`
`table-of-content {enable | disable}`	Disable to not include a table of content at the beginning of each chart category.	`enable`
`title <title_name>`	Enter a name for the report profile.	No default
`title-logo-file <directory_path>`	Enter the path and file name to small logo to use in the title. The logo will be uploaded to the FortiAnalyzer hard disk. When adding a logo to the report, consider the following to ensure you select the correct logo format for the report. If you select a log that is not supported for a report format, the logo will not appear in the report. • PDF reports – JPG and PNG • RTF reports – JPG, PNG, GIF, and WMF • HTML reports – all bitmap formats	No default

config object

Use this sub-command to configure the charts that will be used in the report layout.

```
config object
  edit <obj_id>
    set category [FortiGate{fgt-intrusion | fgt-antivirus |fgt-webfilter |
       fgt-mailfilter | fgt-im | fgt-content | fgt-network | fgt-web | fgt-
       mail | fgt-ftp | fgt-terminal | fgt-vpn | fgt-event | fgt-p2p | fgt-
       voip}] [FortiClient {fct-antivirus | fct-network | fct-webfilter |
       fct-mailfilter}] [FortiMail {fml-highlevel | fml-mail | fml-spam |
       fml-virus}
    set description <comment_str>
    set devices [<device_1> | <device_2> | <device_3> ...]
    set device-mode [variable | specify]
    set filter <filter_name>
    set filter-mode [variable | specify]
    set group <group_name>
    set group-mode [variable | specify]
    set ldap-case-sensitive {enable | disable}
    set ldap-query [enable | disable]
    set ldap-server <server_name>
    set name [<chart_name1> | <chart_name2> | <chart_name3>...]
    set order <integer>
    set period-mode [variable | specify]
    set period-opt [dev | faz]
    set period-type [today | yesterday | last-n-hours | this-week | last-7-
       days | last-n-days | last-2-weeks | last-14-days | this-month | last-
       30-days | last-n-weeks | this-quarter | last-quarter | this-year |
       other]
    set resolve-host [enable | disable]
    set resolve-service [enable | disable]
    set source-id [user | ip | both]
    set style [pie | bar | line]
    set table-graph [all | table | graph]
    set table-top2 <integer>
    set topn <integer>
    set type [chart | section | text]
    set user <user_name>
    set user-mode [variable | specify]
    set vd <virtual_domain_name>
    set vd-mode [variable | specify]
  end
```

Keywords and variables	Description	Default
`edit <obj_id>`	Enter the sequential number for the chart you want to add to the report layout. For example, 1 puts the first configure chart at the top, and 2 puts the second configured chart under the first.	No default
`category [FortiGate{fgt-intrusion | fgt-antivirus |fgt-webfilter | fgt-mailfilter | fgt-im | fgt-content | fgt-network | fgt-web | fgt-mail | fgt-ftp | fgt-terminal | fgt-vpn | fgt-event | fgt-p2p | fgt-voip}] [FortiClient {fct-antivirus | fct-network | fct-webfilter | fct-mailfilter}] [FortiMail {fml-highlevel | fml-mail | fml-spam | fml-virus}`	Enter a chart category. For example, if you are creating a report layout for a FortiGate unit, the `dev-type` would be `FortiGate`, and the charts available to you would be the FortiGate charts, such as `fgt-intrusion` and `fgt-antivirus`. You can chose only the charts available for the chosen device type. For example, if you chose FortiClient, only the charts that are for FortiClient reports are available. After choosing a chart category, you will need to add what charts you want to include in that category. For example, after selecting the `fgt-antivirus` category, you enter `set name ?`, and view all available charts for that category, and select a chart. You can enter only one chart at time.	No default
`description <comment_str>`	Enter a description for when configuring a section or text insert.	No default
`devices [<device_1> | <device_2> | <device_3> ...]`	Enter the specific devices to be included in the report. For example, you want to include both the FortiMail-400 unit and FortiMail-2000 unit. This keyword is available only when `device-mode` is set to `specify`.	No default
`device-mode [variable | specify]`	Enter the device specification mode. If you select specify, the keyword `devices` appears. The keyword `devices` enables you to specify the devices you want to include.	`variable`
`filter <filter_name>`	Enter the filter template name that will be used for the report. This keyword is available only when `filter-mode` is set to `specify`.	No default
`filter-mode [variable | specify]`	Enter to specify if you want to include a specific filter template in the report.	`variable`
`group <group_name>`	Enter the name of the group to include in the report. This keyword is available only when `group-mode` is set to `specify`.	No default
`group-mode [variable | specify]`	Enter to specify if you want to include a specific group in the report.	`variable`
`ldap-case-sensitive {enable | disable}`	Enable the case sensitive setting for LDAP.	`disable`
`ldap-query [enable | disable]`	Enable to add an LDAP server to the report.	`disable`
`ldap-server <server_name>`	Enter the LDAP sever for the report. This keyword is available only when `ldap-query` is enabled.	No default
`name [<chart_name1> | <chart_name2> | <chart_name3>...]`	Enter the name of the charts you want included in that category. You need to enter each chart separately. For example, after `set chart_name1`, you press Enter and then go on to the next name.	No default
`order <integer>`	Enter a number to ensure that the chart is placed in the order you want it to be in.	No default
`period-mode [variable | specify]`	Enter to specify if you want to include a specific time period in the report.	`variable`
`period-opt [dev | faz]`	Enter the time period based on either the device's time or the FortiAnalyzer unit's time. If you choose the FortiAnalyzer unit's time period, the time is when logs were received.	No default

Keywords and variables	Description	Default
`period-type [today | yesterday | last-n-hours | this-week | last-7-days | last-n-days | last-2-weeks | last-14-days | this-month | last-30-days | last-n-weeks | this-quarter | last-quarter | this-year | other]`	Enter the time period that the charts report on. This is available only when `period-mode` is set to `specify`.	No default
`resolve-host [enable | disable]`	Enable to resolve host IP addresses into host names in chart results.	`disable`
`resolve-service [enable | disable]`	Enable to resolve port numbers into service names in chart results.	`disable`
`source-id [user | ip | both]`	Enter to include the source's identity, such as only the user name or only the IP address. You can also choose to have both the user and IP address. This appears if a chart that contains sources is entered.	`both`
`style [pie | bar | line]`	Enter the type of style for the charts. For example, if you select bar, a bar graph displays for the selected charts.	`bar`
`table-graph [all | table | graph]`	Enter to display either a table or a graph.	`all`
`table-top2 <integer>`	Enter a number to show the top Y values in the chart table for the secondary variable.	No default
`topn <integer>`	Enter a number to show the top X values in the chart table for the primary variable. This number can also be the top number of values in the graph. **Note:** When entering a number for the maximum top entries (with pie chart style selected), any item whose percentage is less than one percent will not appear in the pie diagram; also, if no items' percentage is greater than one percent "Other" occupies the pie diagram, or 100 percent of the pie diagram. For example, if you enter the number five, any of the five items that have less than one percent are considered under "Other" and only "Other" displays on the page diagram.	No default
`type [chart | section | text]`	Enter to configure charts, section titles or text inserts for the report layout. When you choose `section` or `text`, only the following are available: • `type` • `order` • `title` • `description`	No default
`user <user_name>`	Enter the name of the user to include in the report. This keyword is available only when `user-mode` is set to `specify`.	No default
`user-mode [variable | specify]`	Enter to specify if you want to include a specific user in the report.	`variable`
`vd <virtual_domain_name>`	Enter the virtual domain that you want included in the report.	No default
`vd-mode [variable | specify]`	Enter to specify if you want to include a specific virtual domain in the report.	`variable`

Example

The following example configures a report layout with one chart and all chart categories included.

```
config report layout
  edit layout_1
```

```
      set title report_1
      set description for_branch_office
      set dev-type FortiGate
      set obfuscate-user enable
      set table-of-content enable
      set company A_company
      set footer-options report-title
      set header-logo-file c:/Company/marketing/marketing_pics/company_pic_1
      set title-logo-file c:/Company/marketing/marketing_pics/company_pic_2
    config object
      edit 1
        set type chart
        set category fgt-intrusion
        set name attacks-type
        set name attacks-cat-type
        set name attacks-ts
        set name attacks-td
        set name attacks-time
        set name attacks-proto
        set name attacks-dir-type
        set name attacks-ips-type
        set name attacks-proto-type
        set name attacks-dir-ip
        set name attacks-type-ip
        set name attacks-dst-ip
        set name attacks-dst-type
        set name attacks-dev-type
        set name attacsk-dev
        set name attacks-type-dev
        set order 3
        set table-graph table
        set style pie
        set topn 5
        set table-top2 10
        set device-mode specify
        set devices FGT-602906512797
        set filter-mode specify
        set filter filter_1
        set include-other enable
        set period-mode specify
        set period-type last-2-weeks
        set period-opt dev
        set resolve-host enable
        set resolve-service enable
      end
    end
```

History

3.0 MR7	New.
4.0 MR1	Removed the keyword `include-referrals`. Added the keyword `ldap-case-sensitive`.

report output

Use this command to configure an output template to be used in a report schedule.

Syntax

```
config report output
  edit <output_name>
    set description
    set email {enable | disable}
    set email-subject <string>
    set email-body <string>
    set email-attachment-name <attachment_name>
    set email-attachment-compress {enable | disable}
    set email-format {html | pdf | rtf | txt | mht | xml}
    set output-format {html | mht | pdf | rtf | txt | xml}
    set upload {enable | disable}
    set upload-server-type {ftp | sfpt | scp}
    set upload-server <class_ip>
    set upload-user <user_name>
    set upload-pass <password>
    set upload-dir <dir_path>
    set upload-delete {disable | enable}
  end
```

Keywords and variables	Description	Default
`edit <output_name>`	Enter a name for the output template.	No default
`description`	Enter a description for the output template. This is optional. If you enter a description, do not use spaces between the words.	No default
`email {enable | disable}`	Enable or disable for sending the report to an email address. All email commands appear after enabling this command.	`disable`
`email-subject <string>`	Enter a subject line for the email.	No default
`email-body <string>`	Enter a message for the body of the email message. You need to separate each word with an underscore (_).	No default
`email-attachment-name <attachment_name>`	Enter a name for the report when it is sent in an email message.	No default
`email-attachment-compress {enable | disable}`	Enable or disable to compress the report when it is sent in an email message.	`disable`
`email-format {html | pdf | rtf | txt | mht | xml}`	Enter the file type of the report when sent in an email message.	`HTML`
`output-format {html | mht | pdf | rtf | txt | xml}`	Enter the format for the report that will be sent out.	No default
`upload {enable | disable}`	Enable or disable to upload the report to a specified server. All other upload commands appear after enabling this command.	`disable`
`upload-server-type {ftp | sfpt | scp}`	Enter the protocol to use when configuring the uploading server.	No default
`upload-server <class_ip>`	Enable or disable to configure a server.	No default
`upload-user <user_name>`	Enter the user name for accessing the server.	No default

Keywords and variables	Description	Default
`upload-pass <password>`	Enter the password for accessing the server.	No default
`upload-dir <dir_path>`	Enter the directory path where the FortiAnalyzer unit saves the generated report on the server.	No default
`upload-delete {disable | enable}`	Enable or disable the option to delete the completed report from the FortiAnalyzer unit's hard disk once it has been completely uploaded to the remote server.	`disable`

Example

The following example configures an output template with uploading to an FTP server.

```
config report output
  edit output_1
    set description forbranchofficeuseonly
    set upload enable
    set upload-server 10.10.16.155
    set upload-server-type ftp
    set upload-user user_1
    set upload-password 2345789
    set upload-dir c:\documents and settings\reports_faz
    set upload-compress enable
  end
```

History

3.0 MR7	New.
4.0 MR1	Removed the keyword `upload-compress` and added `output-format`.

report schedule

Use this command to configure report schedules.

Note: When configuring a report schedule, which contains both an output template and selected file formats, the file formats sent by email are determined by the configuration settings. Only those file formats that are enabled in both the output template and `output-profile` are sent by email. For example, if PDF and Text formats are selected in the output template, and then PDF and MHT are selected in the report schedule, the report's file format in the email attachment is PDF.

Syntax

```
config report schedule
  edit <schedule_name>
    set description <comment_string>
    set layout <reportlayout_name>
    set language <language_name>
    set format {html | pdf | rtf | txt | mht | xml}
    set output-profile <output_name>
    set devices <device_name>
    set vd <virtual_domain_name>
    set user <user_name>
    set group <group_name>
    set ldap-query {enable | disable}
    set ldap-server <ipv4>
    set filter <filter_name
    set type {empheral | demand | once | daily | days | dates}
    set dates {1-31}
    set days {sun | mon | tue | wed | thu | fri | sat}
    set time <hh:mm>
    set valid-start <hh:mm yyyy/mm/dd>
    set valid-end <hh:mm yyyy/mm/dd>
    set period-type {today | yesterday | last-n-hours | this-week | last-7-
       days | last-n-days | last-2-weeks| last-14-days | this-month | last-
       month | last-30-days | last-n-weeks | this-quarter | last-quarter |
       this-year | other}
    set period-opt {dev | faz}
  end
```

Keywords and variables	Description	Default
`edit <schedule_name>`	Enter a name for the schedule.	No default
`description <comment_string>`	Enter a comment or description for the schedule. This is optional.	No default
`layout <reportlayout_name>`	Enter the report profile to be associated with the schedule.	No default
`language <language_name>`	Enter the language that will be associated with the schedule. The default language of the FortiAnalyzer unit displays.	Default language of FortiAnalyzer unit
`format {html | pdf | rtf | txt | mht | xml}`	Enter the format type for the generated report. Fortinet recommends choosing the HTML format because the FortiAnalyzer unit does not send the report unless it is in HTML.	`HTML`
`output-profile <output_name>`	Enter the output template to be associated with the schedule.	No default
`devices <device_name>`	Enter the device name or device group name to report on for the variable charts.	No default
`vd <virtual_domain_name>`	Enter the virtual domain or domains to report on for the variable charts.	No default
`user <user_name>`	Enter the name of the user to report on for the variable charts.	No default
`group <group_name>`	Enter the name of the group on for the variable charts.	No default
`ldap-query {enable | disable}`	Enter enable or disable to use an LDAP query to resolve user names.	`disable`
`ldap-server <ipv4>`	Enter the IP address for the LDAP server. Appears when ldap-query is enabled.	No default
`filter <filter_name`	Enter the filter template to be associated with the report schedule. This is optional.	No default
`type {empheral | demand | once | daily | days | dates}`	Enter the type of schedule that the FortiAnalyzer unit generates the report. For example, if you want the report generated only once, the type is once and if you want the report to be generated on the 5, 7, and 20 of every month, then select dates	`once`
`dates {1-31}`	Available when `dates` is selected for `type`. Enter the dates that the report will be generated on.	No default
`days {sun | mon | tue | wed | thu | fri | sat}`	Available when `days` is selected for `type`. Enter the days of the week that the report will be generated on.	No default
`time <hh:mm>`	Enter the time in the format `hh:mm`.	No default

Keywords and variables	Description	Default
`valid-start <hh:mm yyyy/mm/dd>`	Enter the start date and time for the report schedule.	No default
`valid-end <hh:mm yyyy/mm/dd>`	Enter the end date and time for the report schedule.	No default
`period-type {today | yesterday | last-n-hours | this-week | last-7-days | last-n-days | last-2-weeks| last-14-days | this-month | last-month | last-30-days | last-n-weeks | this-quarter | last-quarter | this-year | other}`	Enter a time period the chart reports are based on.	No default
`period-opt {dev | faz}`	Enter `dev` to base the time period on the selected devices. Enter `faz` to base the time period on when the FortiAnalyzer unit receives the logs from the devices.	No default

Example

The following example configures a report schedule and includes the report profile, filter and output templates.

```
config report schedule
  edit schedule_1
    set layout report_1
    set language English
    set format html pdf
    set output-profile output_1
    set filter filter_1
    set type dates
    set dates 1,5,30
    set time 01:30
    set period-type this-month
    set period-opt dev
  end
```

History

3.0 MR7	New.

report webclick

Web clicks refer to user-requested URLs. Use this command to differentiate webclicks from the non-user-driven web activities that are included in the web logs. For example, you can filter out from the web logs popup advertisements, web redirects, images, and other non-user driven web activities which do not belong to web clicks.

The following criteria helps to determine what is considered a web click when generating a report:

- If there is no previous web log from the same source IP address and user name within a short interval such as two seconds.

- If the file name extensions to the URL of the web log do not match the file types that are specified in the configuration attributes of `file filter` and `custom filter`.
- If the URL does not belong to the advertisement category.

Syntax

```
config report webclick
   set click-interval <integer>
   set custom-filter <string>
   set file-filter [all | all-image| bmp | dib | gif | jpeg | jpg | pct | tif |
      tiff | all-multimedia | asf | asx | avi | flv | mp3 | mpeg | mpg | mov |
      rm | swf | wav | wma | wmv | all-script | css | jss]
   set web-category-filter <string>
end
```

Keywords and variables	Description	Default
`click-interval <integer>`	Specify the time interval when the user clicks the web URL. If there is no previous web log from the same source IP address and user name within the specified time interval, the web activity is deemed as a web click.	`2`
`custom-filter <string>`	Enter a file type that is not listed in `file-filter` below, following the same filename extension format.	No default
`file-filter [all | all-image| bmp | dib | gif | jpeg | jpg | pct | tif | tiff | all-multimedia | asf | asx | avi | flv | mp3 | mpeg | mpg | mov | rm | swf | wav | wma | wmv | all-script | css | jss]`	Enter to filter only specific file types, such as bmp. If you enter `all-image`, you are including all supported images, such as `dib` and `gif`. If you enter `all-multimedia`, you are including all supported media which includes audio, such as `wav`. If you enter `all-script`, you are including `css` and `jss`.	`all`
`web-category-filter <string>`	Enter the web category that will be used to filter the information.	`Advertising`

History

4.0 MR1 New.

sql-report chart

Use this command to configure a customized chart or edit an existing chart for your reports. Before using this command, you must first configure a dataset using "config sql-report dataset" on page 78 because you need a dataset when configuring a chart.

Syntax

```
config sql-report chart
   edit <chart_name>
     set category {AntiVirus | Application_Control | Data_Leak_Prevention |
        Email Filter | Event | Intrusion_Detection | Net_Scan | Network_Monitor
        | Traffic | VPN | VoIP |Web_Filter}
     set dataset <dataset_name>
     set description <string>
     set favorite {enable | disable}
```

```
    set graph-type {bar | pie | table}
    set resolve-hostname {enable | disable}
    set x-axis-data-binding <field_name>
    set x-axis-data-top <top_number_integer>
    set x-axis-label <label_string>
    set y-axis-data-binding <field_name>
    set y-axis-group {enable | disable}
    set y-axis-label <label_string>
  end
```

Keywords and variables	Description	Default
`<chart_name>`	Enter a name for the chart or enter an existing name to edit.	No default
`category {AntiVirus | Application_Control | Data_Leak_Prevention | Email Filter | Event | Intrusion_Detection | Net_Scan | Network_Monitor | Traffic | VPN | VoIP |Web_Filter}`	Select the log category that this chart will use.	No default
`dataset <dataset_name>`	Select a dataset to be used in the chart.	No default
`description <string>`	Enter a comment or description for the chart. The comment or description should contain underscores (_) between each word or quotes, for example, “Report_chart_June_2009”.	No default
`favorite {enable | disable}`	Enable to add the chart to the favorite list. Later on, when you configure the report dashboard, you can add the favorite list to the reports.	`disable`
`graph-type {bar | pie | table}`	Enter the type of graph that will be used in the chart.	`table`
`resolve-hostname {enable | disable}`	Enable to display the device’s host name from an IP alias or reverse DNS lookup, rather than an IP address.	`disable`
`x-axis-data-binding <field_name>`	Enter a value for the x axis of the bar or pie graph. This option is only available when the `graph-type` is `bar` or `pie`.	Varies depending on the dataset selected.
`x-axis-data-top <top_number_integer>`	Enter a number to show the top ranked log information, such as top number of viruses, in the report chart. The rest of the log information will be marked as “Others” in the chart. This option is only available when the `graph-type` is `bar` or `pie`.	10
`x-axis-label <label_string>`	Enter a label to replace the default one for the x axis, if required. This option is only available when the `graph-type` is `bar`.	Varies depending on the dataset selected.
`y-axis-data-binding <field_name>`	Enter a value for the y axis of the bar or pie graph. This option is only available when the `graph-type` is `bar` or `pie`.	Varies depending on the dataset selected.
`y-axis-group {enable | disable}`	Enable or disable grouping the log information on the y-axis according to the data set field output. This option is only available when the `graph-type` is `bar`.	`disable`
`y-axis-label <label_string>`	Enter a label to replace the default one for the y axis, if required. This option is only available when the `graph-type` is `bar`.	Varies depending on the dataset selected.

History

4.0 MR2	New.

sql-report dashboard

Use this command to configure the report dashboard that you can view under *Report* > *Access* on the web-based manager.

Syntax

```
config sql-report dashbooard
  edit widget-id <widget-id>
    set auto-refresh {enable | disable}
    set category {AntiVirus | Application_Control | Data_Leak_Prevention |
       Email | Filter | Event | Intrusion_Detection | Traffic}
    set chart <chart_name>
    set column <colunm_position>{enable | disable}
    set devices <device/device_group>
    set refresh-interval <1-60 minutes>
    set tabid <tab_id>
    set title <dashboard_title>
  end
```

Keywords and variables	Description	Default
`widget-id <widget-id>`	Enter the ID of the widget to configure.	No default
`auto-refresh {enable | disable}`	Enable to refresh the widget automatically.	`enable`
`category {AntiVirus | Application_Control | Data_Leak_Prevention | Email | Filter | Event | Intrusion_Detection | Traffic}`	Select the log category for the report.	No default
`chart <chart_name>`	Enter the chart name that will be used in the report.	No default
`column <colunm_position>{enable | disable}`	Set the widget column number: 1 or 2	`0`
`devices <device/device_group>`	Select the devices or device groups to report on.	No default
`refresh-interval <1-60 minutes>`	Specify an dashboard refresh interval between 1 to 60 minutes.	`0`
`tabid <tab_id>`	Select which dashboard tab to place the widget.	`0`
`title <dashboard_title>`	Enter a title for the dashboard.	No default

History

4.0 MR2	New.

sql-report dashboard-tab

Use this command to add a report dashboard or edit the name of an existing dashboard that you can view under *Report* > *Access* on the web-based manager.

Syntax

```
config sql-report dashbooard-tab
  edit tabid <id>
    set name <name_string>
  end
```

Keywords and variables	Description	Default
`tabid <id>`	Enter the ID of the dashboard to add or edit.	No default
`name <name_string>`	Enter a name for the dashboard.	No default

History

4.0 MR2	New.

sql-report dataset

Use this command to configure datasets that will be used in “config sql-report chart” on page 75. A dataset must be configure first, before configuring a chart, because the chart must contain a dataset.

Before configuring datasets, you need to first go through and find which log type you want to have in your customized dataset. You need to know the log type because you can only have one log type per dataset. When configuring the dataset with the chosen log type, you also need to know which log fields you want to filter for that log type. For example, you choose `app-crtl` and then choose the log fields `app` and `app_type`.

Syntax

```
config sql-report dataset
  edit <dataset_name>
    set log-type {app-crtl | attack | content | dlp | emailfilter | event |
       history | im | none | traffic | virus | voip | webfilter}
    set query <sql_query>
    set time-period {today | yesterday | last-n-hours | this-week | last-7-
       days | last-n-days | last-2-weeks| last-14-days | this-month | last-
       month | last-30-days | last-n-weeks | this-quarter | last-quarter |
       this-year | other}
    set period-last-n <number>
  end
```

Keywords and variables	Description	Default
`<dataset_name>`	Enter a dataset name to add or edit.	No default
`log-type {app-crtl	attack	content	dlp	emailfilter	event	history	im	none	traffic	virus	voip	webfilter}`	Enter a type of log you want for the dataset. You can only choose one log type for each dataset. Multiple log types are not supported. **Note:** You must enter a log type before entering the filter information.	No default

Keywords and variables	Description	Default
`query <sql_query>`	Enter the SQL query. For example: `select kind, src_name, count(*) as totalnum from $log where $filter and app_type='voip' and app='sccp' and action='block' and kind is not null and src_name is not null group by kind, src_name order by totalnum desc limit 100`	No default
`time-period {today | yesterday | last-n-hours | this-week | last-7-days | last-n-days | last-2-weeks| last-14-days | this-month | last-month | last-30-days | last-n-weeks | this-quarter | last-quarter | this-year | other}`	Enter a time period the dataset is based on.	No default
`period-last-n <number>`	If you enter last-n-hours, last-n-days, or last-n-weeks for time period, use this option to define the number of hours, days, or weeks.	No default

History

4.0 MR2	New.

sql-report layout

Use this command to configure the layout for the report to be generated. The report layout includes charts, devices, titles, headers and footers, if applicable.

Syntax

```
config sql-report layout
  edit <layout_name>
    set description <string>
    set display-table-content {enable | disable}
    set output-format {html | mht | pdf | rtf | txt | xml}
    set output-profile <profile_name>
    set schedule {daily | now | weekly}
    set style <string>
    set title <string>
    set subtitle <string>
    config component
      edit <component_id>
        set category {AntiVirus | Application_Control | Data_Leak_Prevention |
           Email | Filter | Event | Intrusion_Detection | Traffic}
        set chart {<chart_name1> | <chart_name2> | <chart_name3>...}
        set devices [<device_1> | <device_2> | <device_3> ...]
        set title <string>
        set type {chart | graphic | heading1 | heading2 | heading3 | page-break
           | text}
    config footer/header
      edit <footer_id_or_header_id>
```

```
        set type {graphic | text}
        set graphic <string>
        set text <string>
end
```

Keywords and variables	Description	Default
`<layout_name>`	Enter a name for the report layout.	No default
`description <string>`	Enter a description for the report layout. This is optional.	No default
`display-table-content {enable | disable}`	Disable to not include a table of content at the beginning of each chart category.	`enable`
`output-format {html | mht | pdf | rtf | txt | xml}`	Enter the output format of the report.	`html`
`output-profile <profile_name>`	Select a profile to use for the report.	No default
`schedule {daily | now | weekly}`	Set the report generating schedule. If you select daily or weekly, also set the hour of the day, and day of the week.	`weekly`
`style <string>`	Select the style to use for the report.	No default
`title <string>`	Enter a title for the report.	No default
`subtitle <string>`	Enter a subtitle of the report.	No default

config component

Use this sub-command to configure the components (charts, graphics, headings, and text) that will be used in the report layout.

```
config component
  edit <component_id>
    set category {AntiVirus | Application_Control | Data_Leak_Prevention |
        Email | Filter | Event | Intrusion_Detection | Traffic}
    set chart {<chart_name1> | <chart_name2> | <chart_name3>...}
    set devices [<device_1> | <device_2> | <device_3> ...]
    set title <string>
    set type {chart | graphic | heading1 | heading2 | heading3 | page-break
        | text}
  end
```

Keywords and variables	Description	Default
`<component_id>`	Enter the sequential number for the component you want to add to the report layout. For example, 1 puts the first configure chart at the top, and 2 puts the second configured chart under the first.	No default
`category {AntiVirus | Application_Control | Data_Leak_Prevention | Email | Filter | Event | Intrusion_Detection | Traffic}`	Select the log category for the report.	No default
`chart {<chart_name1> | <chart_name2> | <chart_name3>...}`	Enter the name of the charts you want included in that category. You need to enter each chart separately. For example, after `set chart_name1`, you press Enter and then go on to the next name.	No default
`devices [<device_1> | <device_2> | <device_3> ...]`	Enter the specific devices to be included in the report. For example, you want to include both the FortiMail-400 unit and FortiMail-2000 unit. This keyword is available only when `device-mode` is set to `specify`.	No default

Keywords and variables	Description	Default
`title <string>`	Enter the title for the component.	No default
`type {chart | graphic | heading1 | heading2 | heading3 | page-break | text}`	Enter the component type.	No default

config footer/header

Use this sub-command to configure the footers and headers that will be used in the report layout.

```
config footer/header
  edit <footer_id_or_header_id>
    set type {graphic | text}
    set graphic <string>
    set text <string>
  end
```

Keywords and variables	Description	Default
`<footer_id_or_header_id>`	Enter the sequential number for the footer/header you want to add to the report layout.	No default
`type {graphic | text}`	Specify the footer/header type: either text or graphic. Then use the below command to specify the text or graphic.	No default
`graphic <string>`	Specify the graphic file name.	No default
`text <string>`	Enter the text.	No default

History

4.0 MR2	New.

system accprofile

Use this command to configure access profiles, which control rights of administrators to access parts of the FortiAnalyzer configuration.

Syntax

```
config system accprofile
  edit <profile_name>
    set admin {none | read | read-write}
    set alerts {none | read | read-write}
    set devices {none | read | read-write}
    set dlp {none | read | read-write}
    set logs {none | read | read-write}
    set net-monitor {none | read | read-write}
    set network {none | read | read-write}
    set quar {none | read | read-write}
    set reports {none | read | read-write}
    set system {none | read | read-write}
    set vuln-mgmt {none | read | read-write}
  end
```

Keywords and variables	Description	Default
`admin {none | read | read-write}`	Set the administrative privilege for the administrative settings.	`none`
`alerts {none | read | read-write}`	Set the administrative privileges for the alert email settings.	`none`
`devices {none | read | read-write}`	Set the administrative privileges for the connected device settings.	`none`
`dlp {none | read | read-write}`	Set the administrative privileges for the DLP archive logs.	`none`
`logs {none | read | read-write}`	Set the administrative privileges for the logs.	`none`
`net-monitor {none | read | read-write}`	Set the administrative privileges for the network analyzer monitor options.	`none`
`network {none | read | read-write}`	Set the administrative privileges for the network traffic reports	`none`
`quar {none | read | read-write}`	Set the administrative privileges for the quarantine options and quarantined files.	`none`
`reports {none | read | read-write}`	Set the administrative privileges for the report configuration	`none`
`system {none | read | read-write}`	Set the administrative privileges for the FortiAnalyzer system configuration settings.	`none`
`vuln-mgmt {none | read | read-write}`	Set the administrative privileges for the vulnerability scanner reports and configuration.	`none`

Example

The following example creates an access account called `report`. The profile enables an administrator to read the various reports from the FortiAnalyzer unit, but cannot modify any configuration.

```
config system accprofile
  edit report
    set devices read-write
    set network read
    set reports read
  end
```

History

3.0 MR2 New command.

3.0 MR3 Removed `sec_event` and `traffic_sum`.
Added `network_summaries`.

3.0 MR4 Added `admin_domains`.

3.0 MR7 Removed the following keywords:

- `admin_domains`
- `forensic`
- `sec_event`

The option write has been removed.

4.0 Removed `vulnerability_scan`, `network_summaries`, and `ip_alias`. Added the keywords `vuln-mgmt` and `net-monitor`.

4.0 MR1 Removed `content` and replaced with `dlp`.

system admin

Use this command to add, edit, and delete administrator accounts.

Use the admin administrator account or an account with system configuration read and write privileges to add new administrator accounts and control their permission levels. Each administrator account except admin administrator must include an access profile. You cannot delete the admin administrator account.

Syntax

```
config system admin
  edit <name_str>
    set accprofile <profile_str>
    set adom <adom_name>
    set email-address <email_addr>
    set first-name <fname_str>
    set last-name <lname_str>
    set mobile-number <cellnum_str>
    set pager-number <pagernum_str>
    set password <password_str>
    set phone-number <phone_str>
    set remote-auth {enable | disable}
    set ssh-public-key1 <pubkey_str>
    set ssh-public-key2 <pubkey_str>
    set ssh-public-key3 <pubkey_str>
    set trusthost1 <remoteaccessip_ipv4> <netmask_ipv4>
    set trusthost2 <remoteaccessip_ipv4> <netmask_ipv4>
    set trusthost3 <remoteaccessip_ipv4> <netmask_ipv4>
  end
```

Keywords and variables	Description	Default
`accprofile <profile_str>`	Enter the access profile to assign to the administrator.	No default.
`adom <adom_name>`	Enter the ADOM that you want the administrator to be associated with.	No default
`email-address <email_addr>`	Enter the email address for the administrator.	No default.
`first-name <fname_str>`	Enter the first name of the administrator.	No default.
`last-name <lname_str>`	Enter the last name of the administrator.	No default.
`mobile-number <cellnum_str>`	Enter the number of the administrator's cell (mobile) phone.	No default.
`pager-number <pagernum_str>`	Enter the number of the administrator's pager.	No default.
`password <password_str>`	Enter a password for the administrator account. For improved security, the password should be at least 6 characters.	No default.
`phone-number <phone_str>`	Enter the phone number of the administrator.	No default.
`remote-auth {enable | disable}`	Select to use a RADIUS server for authentication.	`disable`
`ssh-public-key1 <pubkey_str>`	Enter the user's public key to allow user to login without inputting the admin password. If the configured key matches the public key of the client PC, then the admin does not have to enter a password to log into the FortiAnalyzer unit. If the key does not match, the admin must enter a password.	No default.

Keywords and variables	Description	Default
ssh-public-key2 <pubkey_str>	Enter the user's public key to allow user to login without inputting the admin password.	No default.
ssh-public-key3 <pubkey_str>	Enter the user's public key to allow user to login without inputting the admin password.	No default.
trusthost1 <remoteaccessip_ipv4> <netmask_ipv4>	An IP address or subnet address and netmask from which the administrator can connect to the FortiAnalyzer unit. To enable access to the FortiAnalyzer unit from any address, set one of the trusted hosts to 0.0.0.0 and the netmask to 0.0.0.0.	0.0.0.0 0.0.0.0
trusthost2 <remoteaccessip_ipv4> <netmask_ipv4>	An IP address or subnet address and netmask from which the administrator can connect to the FortiAnalyzer unit. To enable access to the FortiAnalyzer unit from any address, set one of the trusted hosts to 0.0.0.0 and the netmask to 0.0.0.0	0.0.0.0 0.0.0.0
trusthost3 <remoteaccessip_ipv4> <netmask_ipv4>	An IP address or subnet address and netmask from which the administrator can connect to the FortiAnalyzer unit. To enable access to the FortiAnalyzer unit from any address, set one of the trusted hosts to 0.0.0.0 and the netmask to 0.0.0.0	127.0.0.1 255.255.255.255

Example

The following example shows how to add a new administrator account, named jdoe, with a password set to p8ssw0rd and an access profile of reports, with access restricted to a single computer, 192.168.5.4, on the internal network.

```
config system admin
  edit jdoe
    set first_name Jane
    set last_name Doe
    set phone_number 555-2112
    set password p8ssw0rd
    set accprofile reports
    set trusthost1 192.168.5.4 255.255.255.255
  end
```

History

3.0 MR2	Newly revamped with new keywords. permissions keyword removed and replaced with accprofile.
3.0 MR4	Added is-admin, ssh-public-key1, ssh-public-key2, ssh-public-key3, trusthost2, and trusthost3.
3.0 MR7	Removed Admin_Domain and auth-group keywords.

system alert-console

Use this command to set the alert console options for the dashboard.

Syntax

```
config system alert_console
  set period {1 | 2 | 3 | 4 | 5 |6 | 7 }
  set severity_level {information | notify | warning | error | critical |alert
     | emergency}
end
```

Keywords and variables	Description	Default
period {1 | 2 | 3 | 4 | 5 |6 | 7 }	Set the number of days the alert console keeps the alert messages.	No default.
severity_level {information | notify | warning | error | critical |alert | emergency}	Set the alert level to display in the alert console listing.	No default.

Example

You could set alert console to maintain 5 days' worth of warning level alert messages.

```
config system alert_console
  set period 5
  set severity_level warning
end
```

system authgrp

Use this command to add RADIUS authentication servers to an authentication group.

Syntax

```
config system authgrp
  edit <group_str>
    set member <radius_str>
  end
```

Keywords and variables	Description	Default
<group_str>	Enter the name of the authorization group.	No default.
member <radius_str>	Enter a list of the names of RADIUS servers configured in config system radius to the group.	No default.

Example

In this example, two RAIDUS servers are added to an authentication group.

```
config system authgrp
  edit RADIUSGrp
    set member RADIUS1 RADIUS_alt
  end
```

system auto-delete

Use this command to automatically remove report, DLP archives, and local logs at specific times.

Syntax

```
config system auto-delete
    config analyzer-auto-deletion
      set status {enable | disable}
      set value <age_int>
```

```
        set when {days | hours | months | weeks}
    end
      config dlp-files-auto-deletion
        set status {enable | disable}
        set value <age_int>
        set when {days | hours | months | weeks}
    end
      config local-auto-deletion
        set status {enable | disable}
        set value <age_int>
        set when {days | hours | months | weeks}
    end
      config quarantine-files-auto-deletion
        set status {enable | disable}
        set value <age_int>
        set when {days | hours | months | weeks}
    end
      config regular-auto-deletion
        set status {enable | disable}
        set value <age_int>
        set when {days | hours | months | weeks}
    end
      config report-auto-deletion
        set status {enable | disable}
        set value <age_int>
        set when {days | hours | months | weeks}
    end
```

Keywords and variables	Description	Default
`analyzer-auto-deletion`	Enter to configure automatic deletion of Network Analyzer log files.	No default.
`dlp-files-auto-deletion`	Enter to configure automatic deletion of DLP archived files. This command does not delete the associated content logs, which use the same automatic deletion settings as other device log files.	No default.
`local-auto-deletion`	Enter to configure automatic deletion of the FortiAnalyzer unit's own log files.	No default.
`quarantine-files-auto-deletion`	Enter to configure automatic deletion of the quarantine files.	No default
`regular-auto-deletion`	Enter to configure automatic deletion of device log files.	No default.
`report-auto-deletion`	Enter to configure automatic deletion of report files.	No default.
`status {enable | disable}`	Enable or disable automatic file deletion based upon age. If you select `enable`, also configure `value` and `when`.	`disable`
`value <age_int>`	Select a value for the maximum age of files. You will need to also configure `when`. This command appears only when `status` is `enable`.	No default.
`when {days | hours | months | weeks}`	Select the unit of time for the maximum age of the files. You will need to also configure `value`. This command appears only when `status` is `enable`.	No default.

Example

This example shows how set the FortiAnalyzer unit to delete local logs over 40 hours old.

```
config system auto-delete
  config local-auto-deletion
    set status enable
    set when hours
    set value 40
  end
```

History

4.0	New.
4.0 MR1	Changed `content-files-auto-deletion` to `dlp-files-auto-deletion`.

system console

Use this command to configure CLI connections, including the number of lines displayed by the console, and the baud rate.

Syntax

```
config system console
   set baudrate {9600 | 19200 | 38400 | 57600 | 115200}
   set mode {batch | line}
   set output {standard | more}
end
```

Keywords and variables	Description	Default
`baudrate {9600	19200	38400	57600	115200}`	Set the console port baud rate.	`9600`
`mode {batch	line}`	Set the console mode to single line or batch commands.	`line`
`output {standard	more}`	Set console output to standard (no pause) or more (pause after each screen, resume on keypress). This setting applies to `show` or `get` commands only.	`standard`

Example

In this example, the baud rate is set to 38400.

```
config system console
  set baudrate 38400
end
```

system dns

Use this command to set a primary and alternate DNS server address. For features which use domain names, the FortiAnalyzer unit will forward DNS lookups to those IP addresses.

Syntax

```
config system dns
  set primary <dns_ip>
  set secondary <dns_ip>
end
```

Keywords and variables	Description	Default
`primary <dns_ip>`	Enter the primary DNS server IP address.	`0.0.0.0`
`secondary <dns_ip>`	Enter the secondary DNS IP server address.	`0.0.0.0`

Example

In this example, the primary FortiAnalyzer DNS server IP address is set to `172.16.35.133` and the secondary FortiAnalyzer DNS server IP address is set to `172.16.25.132`.

```
config system dns
  set primary 172.16.35.133
  set secondary 172.16.25.132
end
```

system event

Use this command to add, edit, and delete alert events.

Syntax

```
config system event
  edit <event_str>
    set all-devices {select | all}
    set enable-generic-text {yes | no}
    set enable-severity-filter {yes | no}
    set event-time-period <minute>
    set generic-text <string>
    set num-events <integer>
    set severity-filter {high | low | medium | medium-high | medium-low}
    set severity-level-app-crtl-comp {>= | = | <=}
    set severity-level-app-crtl-logs {no check | information | notify |
       warning | error | critical | alert | emrgency}
    set severity-level-attack-comp {>= | = | <=}
    set severity-level-attack-logs {no check | information | notify | warning
       | error | critical | alert | emrgency}
    set severity-level-dlp-comp {>= | = | <=}
    set severity-level-dlp-logs {no check | information | notify | warning |
       error | critical | alert | emrgency}
    set severity-level-emailfilter-comp {>= | = | <=}
    set severity-level-emailfilter-logs {no check | information | notify |
       warning | error | critical | alert | emrgency}
    set severity-level-event-comp {>= | = | <=}
    set severity-level-event-logs {no check | information | notify | warning |
       error | critical | alert | emrgency}
    set severity-level-history-comp{>= | = | <=}
    set severity-level-history-logs {no check | information | notify | warning
       | error | critical | alert | emrgency}
    set severity-level-im-comp {>= | = | <=}
    set severity-level-im-logs {no check | information | notify | warning |
       error | critical | alert | emrgency}
    set severity-level-traffic-comp {>= | = | <=}
    set severity-level-traffic-logs {no check | information | notify | warning
       | error | critical | alert | emrgency}
    set severity-level-virus-comp {>= | = | <=}
    set severity-level-virus-logs {no check | information | notify | warning |
       error | critical | alert | emrgency}
    set severity-level-webfilter-comp {>= | = | <=}
    set severity-level-webfilter-logs {no check | information | notify |
       warning | error | critical | alert | emrgency}
      config alert-destination
        edit <table_index>
          set from <email_str>
          set mail-server-adom
          set smtp-name <server_name>
          set to <email_str>
          set type {mail | snmp | syslog}
        end
  end
```

Keywords and variables	Description	Default
`edit <event_str>`	Enter the name for the alert event.	No default.
`all-devices {select | all}`	Select to watch for events from all devices or from selected devices.	`all`
`enable-generic-text {yes | no}`	Enable to add a standard text response for the alert notification.	`no`
`enable-severity-filter {yes | no}`	Enable the alert severity to include in the outgoing alert message information.	`no`
`event-time-period <minute>`	Select the period of time in minutes when the number of events occur. When the number of events occur in the configured time, the FortiAnalyzer sends an alert email.	`30`
`generic-text <string>`	Enter the standard text response for the alert notification. Use this variable after setting `enable-generic-text` to `yes`.	No default.
`num-events <integer>`	Select the number of events to occur within a configured time period.	`1`
`severity-filter {high | low | medium | medium-high | medium-low}`	Select the alert severity to include in the outgoing alert message information. Use this variable after setting `enable-severity-filter` to `yes`.	No default.
`severity-level-app-crtl-comp {>= | = | <=}`	Select the equivalency in relation to the application control log severity level	`=`
`severity-level-app-crtl-logs {no check | information | notify | warning | error | critical | alert | emrgency}`	Select the severity level that the FortiAnalyzer unit monitors for in the application control logs.	No default
`severity-level-attack-comp {>= | = | <=}`	Select the equivalency in relation to the attack log severity level.	`=`
`severity-level-attack-logs {no check | information | notify | warning | error | critical | alert | emrgency}`	Select the severity level that the FortiAnalyzer unit monitors for in the attack logs.	No default.
`severity-level-dlp-comp {>= | = | <=}`	Select the severity level that the FortiAnalyzer unit monitors for in the Data Leak Prevention logs.	`=`
`severity-level-dlp-logs {no check | information | notify | warning | error | critical | alert | emrgency}`	Select the severity level that the FortiAnalyzer unit monitors for in the Data Leak Prevention logs.	No default
`severity-level-emailfilter-comp {>= | = | <=}`	Select the equivalency in relation to the email filter log severity level.	`=`
`severity-level-emailfilter-logs {no check | information | notify | warning | error | critical | alert | emrgency}`	Select the severity level that the FortiAnalyzer unit monitors for in the email filter logs.	No default.
`severity-level-event-comp {>= | = | <=}`	Select the equivalency in relation to the event log severity level.	`=`

Keywords and variables	Description	Default
`severity-level-event-logs {no check | information | notify | warning | error | critical | alert | emrgency}`	Select the severity level that the FortiAnalyzer unit monitors for in the event logs.	No default.
`severity-level-history-comp{>= | = | <=}`	Select the equivalency in relation to the history log severity level. This is for FortiMail logs.	=
`severity-level-history-logs {no check | information | notify | warning | error | critical | alert | emrgency}`	Select the severity level that the FortiAnalyzer unit monitors for in the history logs. This is for FortiMail logs.	No default
`severity-level-im-comp {>= | = | <=}`	Select the equivalency in relation to the instant message log severity level.	=
`severity-level-im-logs {no check | information | notify | warning | error | critical | alert | emrgency}`	Select the severity level that the FortiAnalyzer unit monitors for in the instant message logs.	No default.
`severity-level-traffic-comp {>= | = | <=}`	Select the equivalency in relation to the traffic log severity level.	=
`severity-level-traffic-logs {no check | information | notify | warning | error | critical | alert | emrgency}`	Select the severity level that the FortiAnalyzer unit monitors for in the traffic logs.	No default.
`severity-level-virus-comp {>= | = | <=}`	Select the equivalency in relation to the virus log severity level.	=
`severity-level-virus-logs {no check | information | notify | warning | error | critical | alert | emrgency}`	Select the severity level that the FortiAnalyzer unit monitors for in the virus logs.	No default.
`severity-level-webfilter-comp {>= | = | <=}`	Select the equivalency in relation to the web filter log severity level.	=
`severity-level-webfilter-logs {no check | information | notify | warning | error | critical | alert | emrgency}`	Select the severity level that the FortiAnalyzer unit monitors for in the web filter logs.	No default.
`alert-destination`	Configure where the FortiAnalyzer unit sends the alert messages.	No default.
`from <email_str>`	Enter the email address where the alert message originates.	No default.
`mail-server-adom`	Enter the virtual domain of the email server.	No default
`smtp-name <server_name>`	Enter the email server name, configured with the command `config system mail.`	No default.

Keywords and variables	Description	Default
`to <email_str>`	Enter the email address where the alert message is destined.	No default.
`type {mail | snmp | syslog}`	Select the type of delivery for the alert message.	`mail`

Example

In this example, a new alert event called `new_event` is added to the warning message of the event logs for all devices. The FortiAnalyzer unit is configured to monitor for two or more events in an hour. The FortiAnalyzer unit is also configured to send a message to the administer using email in this example.

```
config system event
  edit new_event
    set all-devices all
    set event-time-period 1
    set num_events 2
    set severity-level-event-logs warning
      config alert-destination
      edit 0
        set smtp-name companyserver
        set from f_analyzer@example.com
        set to admin@example.com
        set type mail
      end
end
```

Example

This example shows how to change the host name.

```
config system global
  set hostname corporate_logs
end
```

History

3.0 MR7	Added `mail_server_vd` keyword.
4.0	Added `severity-level-dlp-logs` and `severity-level-dlp-comp` keywords.
4.0 MR1	Removed the following keywords: • `severity-level-av-logs` • `severity-level-av-comp` • `severity-level-content-logs` • `severity-level-content-comp` Added the following variable, `no check`.

system fips

Use this command to set the FortiAnalyzer unit into Federal Information Processing Standards-Common Criteria (FIPS-CC) mode. This is an enhanced security mode that is valid only on FIPS-CC-certified versions of the FortiAnalyzer firmware. To get such firmware, contact Fortinet Technical Support.

Note: This command is only available with direct console connection. When you enable FIPS mode, all the existing configuration on the FortiAnalyzer unit is lost.

Syntax

```
config system fips
  set status <enable | disable>
end
```

Keywords and variables	Description	Default
status <enable | disable>	Enable to select FIPS-CC mode operation for the FortiAnalyzer unit.	disable

History

4.0	New.

system fortiguard

Use this command to configure FortiGuard services, including vulnerability management settings, such as proxy server and scheduling of updates of vulnerability management services.

Syntax

```
config system fortiguard
  set fds-override-addr <ip_address>
  set fds-override-enabled [enable | disable]
  set vm-auto-stat [enable | disable]
  set vm-day [sun | mon | tue | wed | thu | fri | sat]
  set vm-frequency [every | daily | weekly]
  set vm-hour <hour>
  set vm-minute <minutes>
  set vm-proxy [enable | disable]
  set vm-proxy-ip <ip_address>
  set vm-proxy-passwd <user_password>
  set vm-proxy-port <port_number>
  set vm-proxy-user <user_name>
  set vm-schedule [enable | disable]
end
```

Keywords and variables	Description	Default
fds-override-addr <ip_address>	Enter the FDS override IP address of the server. This appears only after enabling the FDS override server.	No default
fds-override-enabled [enable | disable]	Enable to configure an FDS override server.	disable
vm-auto-stat [enable | disable]	Enter to disable the automatic report that is generated that is about the state of vulnerability management.	enable
vm-day [sun | mon | tue | wed | thu | fri | sat]	Enter the day, if you chose weekly, for what day of the week that you want vulnerability management services updated.	sun
vm-frequency [every | daily | weekly]	Enter either every or daily to schedule when vulnerability management updates occur.	weekly
vm-hour <hour>	Enter the hour of when to update the vulnerability management services. The hours are from 0-23.	1

Keywords and variables	Description	Default
vm-minute <minutes>	Enter the minute of when to update the vulnerability management services. The minutes are from 0-59.	0
vm-proxy [enable | disable]	Enter to enable the use of SSL proxy server for updating vulnerability services.	disable
vm-proxy-ip <ip_address>	Enter the IP address of the SSL proxy server.	No default
vm-proxy-passwd <user_password>	Enter the user's password for logging in to the SSL proxy server.	No default
vm-proxy-port <port_number>	Enter the port of the SSL proxy server.	8080
vm-proxy-user <user_name>	Enter the user name for logging in to the SSL proxy server.	No default
vm-schedule [enable | disable]	Enable to configure a schedule for updating vulnerability management services.	disable

Example

This example shows how to configure a daily schedule for vulnerabilities and disable the automatically generated vulnerability report.

```
config system fortiguard
  set vm-schedule enable
  set vm-frequency daily
  set vm-hour 5
  set vm-minute 20
  set vm-auto-stat disable
end
```

History

4.0	New.

system global

Use this command to configure global settings that affect basic FortiAnalyzer system configurations.

Syntax

```
config system global
   set admintimeout <timeout_int>
   set adom <enable | disable>
   set backup-compression {high | low | none | normal}
   set backup-managed {enable | disable}
   set ediscovery-quota <number>
   set hostname <host_str>
   set language {english | french | japanese | korean | simch | trach}
   set ldapconntimeout <timeout_int>
   set max-concurrent-users <administrators_int>
   set ntpserver <ntp_ip>
   set ntpsync {enable | disable}
   set remoteauthtimeout <integer>
   set syncinterval <ntpsync_int>
   set timezone <timezone_int>
end
```

Keywords and variables	Description	Default
`admintimeout <timeout_int>`	Set the administrator idle timeout to control the amount of inactive time (in minutes) before the administrator must log in again. The maximum `admintimeout` is 480 minutes (8 hours). To improve security keep the idle timeout at the default value. **Note:** Sessions will not time out when viewing real-time logs.	`5`
`adom <enable | disable>`	Enable or disable the administrative domains mode.	`disable`
`backup-compression {high | low | none | normal}`	Set the speed of compression when backing up a configuration file. The compression speeds are as follows: • `high` – best compression but with the slowest speed • `low` – least compression and is the fastest • `none` – do not compress the file • `normal` – normal compression speed	`normal`
`backup-managed {enable | disable}`	Enable to manage a configuration file during the back up process.	`disabled`
`ediscovery-quota <number>`	Enter the quota in MB of the harddisk space for ediscovery file usage. The size of the reserved space for eDiscovery varies by the total disk space. You cannot adjust the disk quota below the size of the existing eDiscovery results. eDiscovery results will not be saved if they exceed the disk quota.	
`hostname <host_str>`	Type a name for this FortiAnalyzer unit.	`FortiAnalyzer model name.`
`language {english | french | japanese | korean | simch | trach}`	Set the web-based manager display language. You can set `<language>` to one of `english`, `french`, `japanese`, `korean`, `simch` (Simplified Chinese) or `trach` (Traditional Chinese).	`english`
`ldapconntimeout <timeout_int>`	Set the LDAP connection timeout in milliseconds.	`60000`
`max-concurrent-users <administrators_int>`	Set the maximum number of concurrent administrators.	`20`
`ntpserver <ntp_ip>`	Enter the domain name or IP address of a Network Time Protocol (NTP) server.	`10.10.10.1`
`ntpsync {enable | disable}`	Enable or disable automatically updating the system date and time by connecting to a NTP server. For more information about NTP and to find the IP address of an NTP server that you can use, see http://www.ntp.org.	`disable`
`remoteauthtimeout <integer>`	Set the remote authentication timeout value in seconds.	`10`
`syncinterval <ntpsync_int>`	Enter how often, in minutes, the FortiAnalyzer unit should synchronize its time with the NTP server. The `syncinterval` number can be 1 to 1440; 0 disables time synchronization.	`60`
`timezone <timezone_int>`	The number corresponding to your time zone. Press `?` to list time zones and their numbers. Choose the time zone for the FortiGate unit from the list and enter the correct number.	`00`

Example

This example shows how to change the host name.

```
config system global
  set hostname corporate_logs
end
```

History

3.0 MR2	Keywords Admin_Domain, radius-port and remoteauthtimeout added. Keyword refresh changed to refresh_interval.
3.0 MR4	Added command ldapconntimeout.
3.0 MR5	Removed Admin_Domain keyword.
4.0 MR1	Added the keywords `backup-compression` and `backup-managed`. Removed the keyword `refresh`.

system interface

Use this command to edit the configuration of FortiAnalyzer network interfaces.

Syntax

```
config system interface
  edit <interface_str>
    set allowaccess <access_str>
    set fdp {enable | disable}
    set ip <interface_ip>
    set lockout {enable | disable}
    set mtu-override {enable | disable}
    set speed {1000baseT_Full | 100baseT_Full | 100baseT_Half | 10baseT_Full |
       10baseT_Half | Speed_unknown | auto}
    set status {down | up}
end
```

Keywords and variables	Description	Default
`edit <interface_str>`	Edit an existing interface.	No default.
`allowaccess <access_str>`	Enter the types of management access permitted on this interface. Valid types are: • `ping` • `https` • `ssh` • `http` • `telnet` • `aggregator` • `webservice` Separate multiple access types with spaces. If you want to add or remove an option from the list, retype the entire space-delimited list.	Varies by interface.
`fdp {enable | disable}`	Enable or disable to use the Fortinet Discovery Protocol (FDP) for FortiGate units.	`disable`
`ip <interface_ip>`	Enter the interface IP address and netmask. The IP address cannot be on the same subnet as any other interface.	Varies by interface.
`lockout {enable | disable}`	Enable administrator lock out when the administrator fails to log in after three attempts.	`disable`
`mtu-override {enable | disable}`	Enable override of MTU.	`disable`

Keywords and variables	Description	Default
speed {1000baseT_Full | 100baseT_Full | 100baseT_Half | 10baseT_Full | 10baseT_Half | Speed_unknown | auto}	Configure the maximum speed of the interface.	auto
status {down | up}	Start or stop the interface. If the interface is stopped it does not accept or send packets.	up

Example

This example shows how to set a FortiAnalyzer unit's port 1 IP address and netmask to 192.168.100.159 255.255.255.0, and the management access to ping, https, and ssh.

```
config system interface
  edit internal
    set allowaccess ping https ssh
    set ip 192.168.110.26 255.255.255.0
  end
```

History

3.0 MR1	Added lockout and options variables.
3.0 MR3	Added speed command.
4.0	Removed options keyword and added fdp keyword.

system ip-alias

Use this command to add or modify the alias names for IP addresses. When generating reports, the FortiAnalyzer unit displays the alias name rather than the IP address.

Syntax

```
config system ip-alias
  edit <user_str>
    set ip-range <user_ip>
  end
```

Keywords and variables	Description	Default
edit <user_str>	Edit an or add an IP alias entry.	No default.
ip-range <user_ip>	Enter the IP address and netmask or range of addresses.	No default.

Example

This example shows how to add an IP alias for the user User1.

```
config system ip-alias
  edit user1
    set ip-range 10.10.10.1/24
  end
```

system ldap

Use this command to add or modify LDAP or Windows Active Directory servers for features which can look up users, such as reports utilizing LDAP queries.

Syntax

```
config system ldap
  edit <ldap_string>
    set cnid <cnid_str>
    set dn <dn_str>
    set filter <filter_criteria>
    set group <name_str>
    set password <password_str>
    set port <port_int>
    set server <server_ipv4>
    set type {anonymous | regular}
    set username <username_str>
  end
```

Keywords and variables	Description	Default
`cnid <cnid_str>`	Enter the Common Name Identifier.	`cn`
`dn <dn_str>`	Enter the Distinguished Name information.	No default.

`filter <filter_criteria>`	Enter a filter criteria. This is used for group searching. For example:
	`(&(objectcategory=group)(member=*))`
	`(&(objectclass=groupofnames)(member=*))`
	`(&(objectclass=groupofuniquenames)(uniquemember=*))`
	`(&(objectclass=posixgroup)(memberuid=*))`
		`(&(objectcategory=group)(member=*))`

`group <name_str>`	Enter a group name.	No default.
`password <password_str>`	If `type` is `regular`, enter the Bind password. This option only appears when `type` is `regular`.	No default.
`port <port_int>`	Enter the server port, typically port 389.	`389`
`server <server_ipv4>`	Enter the LDAP server domain name or IP address.	No default.
`type {anonymous | regular}`	Select the server's LDAP binding type. If `type` is `regular`, you must also configure `username` and `password`.	`anonymous`
`username <username_str>`	If `type` is `regular`, enter the Bind Distinguished Name. This option only appears when `type` is `regular`.	No default.

Example

The following example configures an LDAP server connection to `ldap.example.com`.

```
config system ldap
  edit 1
    set server ldap.example.com
    set type regular
    set username faz100
    set set password $32659*fdsQeV
  end
```

History

3.0 MR4	New command.
3.0 MR7	Removed `username` and `password` keywords.
4.0	Removed `secure and ca-cert` keywords.

system mail

Use this command to add or modify an email server user to enable the FortiAnalyzer to send alert messages using email.

Syntax

```
config system mail
  edit <server_name>
    set auth {enable | disable}
    set passwd <password_str>
    set user <user_address>
  end
```

Keywords and variables	Description	Default
`<server_name>`	The name/address of the SMTP email server.	No default.
`auth {enable | disable}`	Select enable to define the email server for alert messages.	`disable`.
`passwd <password_str>`	Enter the password for logging on to the SMTP server to send alert email. You only need to do this if you selected SMTP authentication.	No default.
`user <user_address>`	Enter the user email address for logging on to the SMTP server to send alert mails. You need to do this only if you have enabled the SMTP authentication.	No default.

Example

This example shows how to add SMTP mail server.

```
config system mail
  edit smtp.server.com
    set auth enable
    set user admin@smtp.server.com
    set passwd s3cr3t
  end
```

system migration

Use this command to migrate data from one FortiAnalyzer unit to another.

Syntax

```
config system migration
  set archives {enable | disable}
  set e-discovery {enable | disable}
  set ips {enable | disable}
```

```
   set logs {enable | disable}
   set logs-db {enable | disable}
   set nas {enable | disable}
   set net-analyzer {enable | disable}
   set password <peer_password>
   set peer <ipv4_address>
   set quarantine {enable | disable}
   set reports {enable | disable}
   set role {destination | source}
   set rx-data {enable | disable}
   set status {enable | disable}
   set unreg-dlp-quar {enable | disable}
   set unreg-logs-and-db {enable | disable}
end
```

Keywords and variables	Description	Default
archives {enable | disable}	Enable archive files for migration.	enable
e-discovery {enable | disable}	Enable e-discovery files for migration.	enable
ips {enable | disable}	Enable IPS packet logs for migration.	enable
logs {enable | disable}	Enable log files for migration.	enable
logs-db {enable | disable}	Enable the log database file for migration.	enable
nas {enable | disable}	Enable the network sharing files for migration.	enable
net-analyzer {enable | disable}	Enable the net-analyzer log migration.	enable
password <peer_password>	Enter the “admin” user password of the source FortiAnalyzer unit which sends out data. The destination FortiAnalyzer unit needs to use this password to log on to the source unit.	No default
peer <ipv4_address>	The IP address of the FortiAnalyzer unit that is sending the data, or receiving the data, whichever is that FortiAnalyzer unit’s designation for migration.	0.0.0.0
quarantine {enable | disable}	Enable quarantine files for migration.	enable
reports {enable | disable}	Enable reports for migration.	enable
role {destination | source}	Enter the role that the FortiAnalyzer unit will play in the migration process.	No default
rx-data {enable | disable}	Enable to receive logs on the destination FortiAnalyzer unit while migrating data.	disable
status {enable | disable}	Enable to begin configuration of migration settings.	disable
unreg-dlp-quar {enable | disable}	Enable unregistered DLP and quarantine files for migration.	enable
unreg-logs-and-db {enable | disable}	Enable unregistered device log migration. This allows unregistered devices to send logs during the migration process.	enable

Example

This example shows how to configure a FortiAnalyzer unit to migrate data from that unit to another FortiAnalyzer unit.

On the destination FortiAnalyzer unit:

```
   config system migration
```

```
    set status enable
    set role destination
    set peer 172.16.144.122
    set quarantine enable
    set reports enable
    set logsdb enable
  end
```

On the source FortiAnalyzer unit:

```
  config system migration
    set status enable
    set role source
    set peer 172.16.154.10
  end
```

History

4.0 MR1	New.

system radius

Use the these commands to configure a RADIUS authentication server.

Syntax

```
config system radius
  edit <raidus_name>
    set auth-prot {auto | mschap | mmschap2 | chap | pap}
    set port <udp_port>
    set secret <password_str>
    set server <nameip_str>
  end
```

Keywords and variables	Description	Default
auth-prot {auto | mschap | mmschap2 | chap | pap}	Select which protocol to use when communicating with the RADIUS server.	No default
port <udp_port>	Enter the UDP port number.	No default
secret <password_str>	Enter the password for the RADIUS server.	No default.
server <nameip_str>	Enter the RADIUS server domain name or IP address.	No default.

Example

This example shows how to add a RADIUS server named `corporate` and specify the CHAP protocol on port 1811.

```
config system radius
  edit corporate
    set server 10.10.20.155
    set secret pa55w0rd
    set auth-prot chap
    set port 1811
  end
```

History

3.0 MR2	New command.
3.0 MR5	Added `radius-port`, `specified_proto` and `use_default_auth`.
3.0 MR6	Removed variable `use_default_auth`. The configured RAIDUS protocol is now always used.
4.0	Removed `specified_proto` and `radius-port`. Added the following: • `auth-prot` • `port`

system raid

Use the this command to configure RAID levels.

Syntax

```
config system raid
  set level [raid10 | linear | raid0 | raid1 | raid5]
end
```

Keywords and variables	Description	Default
`level [raid10 | linear | raid0 | raid1 | raid5]`	Enter the level of RAID you want for your FortiAnalyzer unit.	No default

Example

This example shows how configure the RAID level on a FortiAnalyzer unit.

```
config system raid
  set level raid1
end
```

History

4.0	New.

system route

Use the these commands to configure static routes.

Syntax

```
config system route
  edit <sequence_int>
    set device {port1 | port2 | port3}
    set dst <destination_ip-mask>
    set gateway <gateway_ip>
  end
```

Keywords and variables	Description	Default
`edit <sequence_int>`	Enter a sequence number for the static route. The sequence number may influence routing priority in the FortiGate forwarding table.	No default.
`device {port1 | port2 | port3}`	Enter the interface for the outbound packets	`port1`
`dst <destination_ip-mask>`	Enter the destination IP address and network mask for this route. You can enter `0.0.0.0 0.0.0.0` to create a new static default route.	`0.0.0.0 0.0.0.0`
`gateway <gateway_ip>`	Enter the IP address of the next-hop router to which traffic is forwarded.	`0.0.0.0`

Example

This example shows how to add a static route that has the sequence number 2.

```
config system route
  edit 2
    set device port1
    set dst 192.168.22.0 255.255.255.0
    set gateway 192.168.22.44
  end
```

system snmp

Use this command to configure the SNMP server for alert messages.

Syntax

```
config system snmp community
  edit <snmp_name>
    set events {cpu-high | mem-low | log-full | intf-ip | vpn-tun-up | vpn-
       tun-down | system_event | raid | log-rate | data-rate}
    set query-v1-port <port_number>
    set query-v1-status [enable | disable]
    set query-v2c-port <port_number>
    set query-v2c-status [enable | disable]
    set status {enable | disable]
    set trap-v1-lport <port_number>
    set trap-v1-rport <port_number>
    set trap-v1-status {enable | disable}
    set trap-v2c-lport <port_number>
    set trap-v2c-rport <port_number>
    set trap-v2c-status {enable | disable}
  end
```

Keywords and variables	Description	Default
events {cpu-high | mem-low | log-full | intf-ip | vpn-tun-up | vpn-tun-down | system_event | raid | log-rate | data-rate}	Enter the event or events. If you are entering multiple events, you need to have a space between each event.	No default
query-v1-port <port_number>	Enter the SNMP query port number.	161
query-v1-status [enable | disable]	Enable the SNMP v1 query.	enable
query-v2c-port <port_number>	Enter the SNMP query port number.	161
query-v2c-status [enable | disable]	Disable to not configure SNMP v2c query.	enable
status {enable | disable]	Enable to configure an SNMP community	disable
trap-v1-lport <port_number>	Enter the SNMP v1 trap local port number.	162
trap-v1-rport <port_number>	Enter the SNMP v1 remote port number.	162
trap-v1-status {enable | disable}	Disable to not configure the SNMP v1 trap.	enable
trap-v2c-lport <port_number>	Enter the SNMP v2c trap local port number.	162
trap-v2c-rport <port_number>	Enter the SNMP v2c trap remote port number.	162
trap-v2c-status {enable | disable}	Disable to not configure the SNMP v2c trap.	enable

```
config system snmp sysinfo
  set agent {enable | disable}
  set contact-info<info_str>
  set description <desc_str>
  set location <location_str>
end
```

Keywords and variables	Description	Default
agent {enable | disable}	Enable the SNMP agent.	disable
contact-info<info_str>	Enter an administrative contact for the SNMP server.	No default.
description <desc_str>	Enter a description for the server.	No default.
location <location_str>	Enter the location of the server.	No default.

```
config system snmp traps {cpu | memory | disk}
  set frequency <integer>
  set period <integer>
  set threshold <integer>
  set trigger <integer>
end
```

Keywords and variables	Description	Default
traps {cpu | memory | disk}	Enter to configure traps for CPU, Memory or Disk.	No default
frequency <integer>	Enter a time period, in seconds, for the frequency of the traps that occur.	No default
period <integer>	Enter a time period, in seconds.	No default

Keywords and variables	Description	Default
`threshold <integer>`	Enter a number for the number of triggers that occur before sending a trap.	No default
`trigger <integer>`	Enter a percentage that will trigger a trap. The number can be from 1 to 100 (in percent).	No default

Example

This example shows how to add an SNMP server.

```
config system snmp community
  edit snmp_server1
    set community company_snmp
  end
    config system snmp sysinfo
      set contact_info Johnny_admin
      set description corporate_trap
      set location HQ
    end
```

History

3.0 MR2	`config system snmp sysinfo` commands added.
3.0 MR7	Added the following keywords to snmp community: • `traps` • `cpu_usage` • `memory_usage` • `disk_usage` • `system_event` • `intf_ip_change` • `hosts` Removed the keyword, ip from `snmp community` command. Added the following keyword to `snmp sysinfo` command: • `agent` Added the following command and keywords: • `snmp traps {cpu | memory | disk}` • `trigger` • `threshold` • `period` • `frequency`

system sql

Use the these commands to configure the SQL database options.

The FortiAnalyzer unit supports both local PostgreSQL and remote MySQL database options.

The logs received by the FortiAnalyzer unit will be inserted into the SQL database for generating reports. The advantages of using the SQL database are:

- Flexibility: Through the use of standard SQL queries, more flexible reporting capabilities can be offered.
- Scalability: Through the use of a remote SQL database, any upper bound on the amount of available log storage is removed. Furthermore, the hardware of an external SQL database server can be more easily upgraded to support growing performance needs.

Syntax

```
config system sql
   set status {disable | local | remote}
   set database-type <postgres>
   set logtype {app-ctrl | attack | content | dlp | emailfilter | event |
       |netscan | none | traffic | virus | webfilter}
   set start-time <hh:mm> <yyyy/mm/dd>
   set database-name <string>
   set database-type <mysql>
   set set password <password>
   set server <ip_or_hostname>
   set set username <user_name>
end
```

Keywords and variables	Description	Default
`status {disable | local | remote}`	• `disable`: Disable the SQL databases. Logs will be stored in the FortiAnalyzer unit's own storage system. • `local`: Enable the local SQL database. • `remote`: Enable the remote SQL database.	`disable`
If status is set to local, configure the following options:		
`database-type <postgres>`	Specify the SQL database type. Currently, only PostgreSQL is supported.	`postgres`
`logtype {app-ctrl | attack | content | dlp | emailfilter | event | |netscan | none | traffic | virus | webfilter}`	Enter a log type to send to the selected SQL database.	All types.
`start-time <hh:mm> <yyyy/mm/dd>`	Enter the date and time to start sending logs to the selected SQL database.	The current time.
If status is set to remote, configure the following options:		
`database-name <string>`	Enter the remote SQL database name.	
`database-type <mysql>`	Currently, only MySQL is supported.	`mysql`
`logtype {app-ctrl | attack | content | dlp | emailfilter | event | |netscan | none | traffic | virus | webfilter}`	Enter a log type to send to the selected SQL database.	All types.
`password <password>`	Enter the password used to log on to the remote database.	
`server <ip_or_hostname>`	Enter the IP address or host name of the remote database.	
`start-time <hh:mm> <yyyy/mm/dd>`	Enter the date and time to start sending logs to the selected SQL database.	The current time.
`username <user_name>`	Enter the user name used to log on to the remote database.	

Example

This example shows how to select a log type to send to the SQL database.

```
config system sql
  set logtype app-control
end
```

History

4.0 MR2	New.

system syslog

Use the these commands to configure the syslog server for alert messages.

Syntax

```
config system syslog
  edit <syslog_str>
    set ip <ip-address_fdqn>
    set port <name_str>
  end
```

Keywords and variables	Description	Default
`<syslog_str>`	Enter a name for the syslog server.	No default.
`ip <ip-address_fdqn>`	Enter the syslog server IP address and network mask or fully qualified domain name (FQDN).	No default.
`port <name_str>`	Enter the port number for the syslog messages.	No default.

Example

This example shows how to add a Syslog server.

```
config system syslog
  edit syslog1
    set ip syslog.example.com
    set port 514
  end
```

History

3.0 MR2	New.

vm asset-group

Before hosts can be scanned, they must be grouped. These groups are then selected within network map configuration profiles and scan schedules. Grouping hosts eliminates the need to select every host in each scan profile. When your groups have been created, simply specify the required group in the scan profile. Hosts can be included in multiple groups.

Syntax

```
config vm asset-group
  edit <group_str>
    set comment <string>
    set division <string>
    set function <string>
    set host <host_str> [<host_str> <host_str>...]
    set impact-level {low | minor | medium | high | critical}
    set location <string>
```

```
end
```

Variables	Description	Default
`<group_str>`	Enter the name of the asset group you want to edit. To create a new asset group, enter a new name.	No default
`comment <string>`	Enter an optional description of the asset group.	No default
`division <string>`	Enter the division the asset group is a part of. This is an optional information-only field.	No default
`function <string>`	Enter the function of the asset group. This is an optional information-only field.	No default
`host <host_str> [<host_str> <host_str>...]`	Enter the hosts that are in the asset group. Separate multiple hosts with spaces. Enter `set host ?` to list the available hosts.	No default
`impact-level {low | minor | medium | high | critical}`	A rating indicating the relative importance of the hosts in the group.	`high`
`location <string>`	Enter the location of the asset group. This is an optional information-only field.	No default

Example

This example details the commands required to define an asset group called `all-servers`. The asset group contains three hosts previously defined with the host-asset command. The three hosts are named `email-server`, `web-server`, and `db-server`. The asset group is assigned a `high` impact-level and a function of “all servers”.

```
config vm asset-group
  edit all-servers
    set function "all servers"
    set impact-level high
    set host email-server web-server db-server
  end
```

History

4.0	New.

Related commands

- vm host-asset

vm business-risk

The business risk table values form the basis of the business risk calculation, used to order the Top 10 Vulnerable Hosts list located in *Vulnerability Mgmt > Summary > Host Status*. The calculation uses the severity of the detected vulnerabilities, the business impact you assigned to the asset group, and the business risk table.

When creating an asset group, you assign it a business impact:

- low
- minor
- medium

- high
- critical

Vulnerabilities are rated by severity and each severity has a numeric security risk value:

- information: 1
- low: 2
- medium: 3
- high: 4
- critical: 5

To determine the business risk of the host, a look-up is performed. The security risk and the business impact are compared and the appropriate value is taken from the business risk table. For example, if a medium severity vulnerability is found on a host in an asset group with a critical business impact, the business risk table indicates a business risk of 36.

If multiple vulnerabilities are discovered when scanning the host, the default behavior is to average the security risk ratings. With the business impact, this security risk average is used to determine the business risk. If the security risk is not a whole number, the fractional value is used to determine the same fractional value between the two nearest business risk values.

For example, if a medium and a high severity vulnerability are discovered on a medium business impact host, the security risk value is 3.5. A security risk of 3 and a medium business impact result in a business risk of 9, while a security risk of 4 and a medium business impact result in a business risk of 16. The security risk average of 3.5 falls half way between 3 and 4, therefore the business risk falls half way between 9 and 16, which is 12.5. The report will drop all decimals so the final business risk is 12.

The `security-risk` command can be used to instead report the highest security risk found rating rather than the average of all of them. If the `security risk` command is set to `highest` for the example above, the security risk values of the two vulnerabilities would not be averaged. Rather the highest would be used, which is 4, resulting in a business risk of 16.

Use the `business-risk` command to change the values in the table, and therefore the security risk result.

Syntax

```
config vm business-risk
  edit DEFAULT
    set security-risk {average | highest}
    set low-1 <risk_int>
    set low-2 <risk_int>
    set low-3 <risk_int>
    set low-4 <risk_int>
    set low-5 <risk_int>
    set minor-1 <risk_int>
    set minor-2 <risk_int>
    set minor-3 <risk_int>
    set minor-4 <risk_int>
    set minor-5 <risk_int>
    set medium-1 <risk_int>
    set medium-2 <risk_int>
    set medium-3 <risk_int>
    set medium-4 <risk_int>
    set medium-5 <risk_int>
    set high-1 <risk_int>
    set high-2 <risk_int>
    set high-3 <risk_int>
```

```
        set high-4 <risk_int>
        set high-5 <risk_int>
        set critical-1 <risk_int>
        set critical-2 <risk_int>
        set critical-3 <risk_int>
        set critical-4 <risk_int>
        set critical-5 <risk_int>
    end
```

Variables	Description	Default
DEFAULT	Enter the business risk table. Currently, all FortiAnalyzer models support only one table named DEFAULT.	
security-risk {average | highest}	Specify how the security risk is calculated. Either by the average security level or the highest security level.	average
low-1 <risk_int>	Enter the business risk value when the business impact is low and the security risk is 1. The valid range for <risk_int> is 0 to 100.	1
low-2 <risk_int>	Enter the business risk value when the business impact is low and the security risk is 2. The valid range for <risk_int> is 0 to 100.	1
low-3 <risk_int>	Enter the business risk value when the business impact is low and the security risk is 3. The valid range for <risk_int> is 0 to 100.	2
low-4 <risk_int>	Enter the business risk value when the business impact is low and the security risk is 4. The valid range for <risk_int> is 0 to 100.	4
low-5 <risk_int>	Enter the business risk value when the business impact is low and the security risk is 5. The valid range for <risk_int> is 0 to 100.	9
minor-1 <risk_int>	Enter the business risk value when the business impact is minor and the security risk is 1. The valid range for <risk_int> is 0 to 100.	1
minor-2 <risk_int>	Enter the business risk value when the business impact is minor and the security risk is 2. The valid range for <risk_int> is 0 to 100.	2
minor-3 <risk_int>	Enter the business risk value when the business impact is minor and the security risk is 3. The valid range for <risk_int> is 0 to 100.	4
minor-4 <risk_int>	Enter the business risk value when the business impact is minor and the security risk is 4. The valid range for <risk_int> is 0 to 100.	9
minor-5 <risk_int>	Enter the business risk value when the business impact is minor and the security risk is 5. The valid range for <risk_int> is 0 to 100.	16
medium-1 <risk_int>	Enter the business risk value when the business impact is medium and the security risk is 1. The valid range for <risk_int> is 0 to 100.	2
medium-2 <risk_int>	Enter the business risk value when the business impact is medium and the security risk is 2. The valid range for <risk_int> is 0 to 100.	4
medium-3 <risk_int>	Enter the business risk value when the business impact is medium and the security risk is 3. The valid range for <risk_int> is 0 to 100.	9
medium-4 <risk_int>	Enter the business risk value when the business impact is medium and the security risk is 4. The valid range for <risk_int> is 0 to 100.	16
medium-5 <risk_int>	Enter the business risk value when the business impact is medium and the security risk is 5. The valid range for <risk_int> is 0 to 100.	36
high-1 <risk_int>	Enter the business risk value when the business impact is high and the security risk is 1. The valid range for <risk_int> is 0 to 100.	4
high-2 <risk_int>	Enter the business risk value when the business impact is high and the security risk is 2. The valid range for <risk_int> is 0 to 100.	9
high-3 <risk_int>	Enter the business risk value when the business impact is high and the security risk is 3. The valid range for <risk_int> is 0 to 100.	16
high-4 <risk_int>	Enter the business risk value when the business impact is high and the security risk is 4. The valid range for <risk_int> is 0 to 100.	36

Variables	Description	Default
`high-5 <risk_int>`	Enter the business risk value when the business impact is high and the security risk is 5. The valid range for `<risk_int>` is `0` to `100`.	`64`
`critical-1 <risk_int>`	Enter the business risk value when the business impact is critical and the security risk is 1. The valid range for `<risk_int>` is `0` to `100`.	`9`
`critical-2 <risk_int>`	Enter the business risk value when the business impact is critical and the security risk is 2. The valid range for `<risk_int>` is `0` to `100`.	`16`
`critical-3 <risk_int>`	Enter the business risk value when the business impact is critical and the security risk is 3. The valid range for `<risk_int>` is `0` to `100`.	`36`
`critical-4 <risk_int>`	Enter the business risk value when the business impact is critical and the security risk is 4. The valid range for `<risk_int>` is `0` to `100`.	`64`
`critical-5 <risk_int>`	Enter the business risk value when the business impact is critical and the security risk is 5. The valid range for `<risk_int>` is `0` to `100`.	`100`

History

4.0	New.

Related commands

- vm asset-group
- vm schedule

vm host-asset

The host-asset command allows you to define your organizations hosts. Hosts not appearing on this list can not be included in asset groups.

Syntax

```
config vm host-asset
  edit <asset_str>
    set auth {snmp | unix | windows}
    set auth-level {domain | local}
    set comment <string>
    set community-string <string>
    set dsa-key <key_str>
    set function <string>
    set ip <ipv4[-<ipv4>]>
    set location <string>
    set rsa-key <key_str>
    set sudo {enable | disable}
    set tag <string>
    set unix-password <pass_str>
    set unix-user-name <id_str>
    set win-password <pass_str>
    set win-user-name <id_str>
  end
```

Variables	Description	Default
`<asset_str>`	Enter the name of the asset you want to edit. To create a new asset, enter a new name.	
`auth {snmp | unix | windows}`	To allow the FortiAnalyzer to authenticate with the host during VM scans, enter the authentication type. Depending on the authentication type, other commands will appear allowing you to enter the appropriate information. Use the command `unset auth` to remove authentication.	
`auth-level {domain | local}`	Select whether Windows authentication is local or domain-based. This command is available when the `auth` keyword is set to `windows`.	`local`
`comment <string>`	Enter an optional description of the host-asset profile.	No default
`community-string <string>`	Enter the SNMP community. This command appears only when `auth` is set to `snmp`.	No default
`dsa-key <key_str>`	Enter the PEMencoded private key in text format. This command appears only when `auth` is set to `unix`.	No default
`function <string>`	Enter the function of the host. This is an optional information-only field.	No default
`ip <ipv4[-<ipv4>]>`	Enter the host IP address. You can enter an IP range by separating the start and end addresses with a dash.	No default
`location <string>`	Enter the location of the host. This is an optional information-only field.	No default
`rsa-key <key_str>`	Enter the PEMencoded private key in text format. This command appears only when `auth` is set to `unix`.	No default
`sudo {enable | disable}`	Enable to give the FortiAnalyzer UNIX super-user privileges. This command appears only when `auth` is set to `unix`.	`disable`
`tag <string>`	Enter the asset tag of the host. This is an optional information-only field.	No default
`unix-password <pass_str>`	Enter the password the FortiAnalyzer uses to authenticate with the UNIX host. This command appears only when `auth` is set to `unix`.	No default
`unix-user-name <id_str>`	Enter the username the FortiAnalyzer uses to authenticate with the UNIX host. This command appears only when `auth` is set to `unix`.	No default
`win-password <pass_str>`	Enter the password the FortiAnalyzer uses to authenticate with the Windows host. This command appears only when `auth` is set to `windows`.	No default
`win-user-name <id_str>`	Enter the username the FortiAnalyzer uses to authenticate with the Windows host. This command appears only when `auth` is set to `windows`.	No default

Example

This example details the commands required to define a host-asset called `email-server`. The host is at IP address 172.20.120.200 and the optional `function` and `location` commands indicate that it is an email server on the third floor.

```
config vm host-asset
  edit email-server
    set ip 172.20.120.200
    set location "third floor"
    set set function "email server"
  end
```

History

4.0	New.

Related commands

- vm asset-group

vm map-config

Network map reports are generated based on network map configuration profiles. Multiple profiles can be created to make reports containing only the required information.

Syntax

```
config vm map-config
  edit <config_str>
    set approved-host <ipv4> [<ipv4> <ipv4>...]
    set asset-group <grp_str>
    set date <date_str>
    set domain <domain_str>
    set exclude-dns-only-host {enable | disable}
    set format {html mht pdf rtf txt}
    set grp-update {enable | disable}
    set hour <hour_int>
    set ip-range <ipv4>
    set live-host-sweep {enable | disable}
    set max-occurrence <max_int>
    set minute <minute_int>
    set output-profile <profile_str>
    set recurrence {daily | weekly | monthly}
    set schedule {run-now | run-later}
    set tcp-port-adtn <string>
    set tcp-standard-scan {enable | disable}
    set udp-standard-scan {enable | disable}
  end
```

Variables	Description	Default
`<config_str>`	Enter the name of the map configuration you want to edit. To create a new map configuration, enter a new name.	No default
`approved-host <ipv4> [<ipv4> <ipv4>...]`	Enter the IP addresses of approved hosts. Enter multiple addresses separated by spaces.	No default
`asset-group <grp_str>`	Enter the asset group on which the network map scan will run.	No default
`date <date_str>`	Enter the date a scheduled scan will start. The date must be formatted as a four digit year, a two digit month, and a two digit day, each separated by a dash. For example, `2009-12-01` would be formatted properly. If left blank, the schedule will start on the current day, subject to the schedule itself.	No default
`domain <domain_str>`	Enter a domain name in which the scan will be executed.	No default
`exclude-dns-only-host {enable | disable}`	Enable to exclude hosts discovered only in the DNS.	`disable`
`format {html mht pdf rtf txt}`	Enter the required output format or formats of the map report.	`html`

Variables	Description	Default
grp-update {enable | disable}	Enable to have the network map scan automatically update the specified asset group if new hosts are discovered. No hosts will be removed even if they unreachable. A domain or IP range must be entered if grp-update is enabled. You must specify an asset group with the asset-group command before configuring this setting.	disable
hour <hour_int>	Specify when during the day a scheduled scan will run. Use this command with minute to specify an exact time.	12
ip-range <ipv4>	Enter the IP address range the FortiAnalyzer scans.	No default
live-host-sweep {enable | disable}	Enable to have the FortiAnalyzer discover live hosts in the IP address range specified with the ip-range command.	enable
max-occurrence <max_int>	Enter the maximum number of times this scheduled scan runs. Enter 0 for no maximum.	0
minute <minute_int>	Specify when during the day a scheduled scan will run. Use this command with hour to specify an exact time.	0
output-profile <profile_str>	Enter the report output profile name.	No default
recurrence {daily | weekly | monthly}	Enter how often a scheduled scan is run. • daily has the FortiAnalyzer run the scan once a day. Use the hour and minute commands to specify when during the day the scan is run. • weekly has the FortiAnalyzer run the scan once a week. Use the day-of-week, hour, and minute commands to specify when during the week the scan is run. • monthly has the FortiAnalyzer run the scan once a month. Use the day-of-month, hour, and minute commands to specify when during the month the scan is run.	daily
schedule {run-now | run-later}	Specify whether the schedule will run once or at regular intervals. • run-now will have the FortiAnalyzer run the specified map configuration immediately, and only once. • run-later will have the FortiAnalyzer run the map configuration at regular intervals, as specified with the recurrence command.	run-now
tcp-port-adtn <string>	Enter any ports you want scanned in addition to those specified with the tcp-standard-scan command. Enter individual ports separating by commas. Enter port ranges, separating the start and end ports with a dash. For example, set tcp-port-adtn 10,12,14,20-30	No default
tcp-standard-scan {enable | disable}	Enable to scan 13 standard TCP ports: 21-23, 25, 53, 80, 88, 110, 111, 135, 139, 443, 445.	enable
udp-standard-scan {enable | disable}	Enable to scan 6 standard UDP ports: 53, 11, 135, 137, 161, 500.	disable

Example

This example details the commands required to create a map-config named servers. This map-config will scan the all-servers asset-group daily at 1 A.M. every day.

```
config vm map-config
  edit servers
    set asset-group all-servers
    set domain example.com
    set grp-update disable
    set schedule run-later
    set recurrence daily
    set hour 1
    set minute 0
  end
```

History

4.0 New.

Related commands

- vm asset-group

vm scan-profile

Scan profiles are used to define exactly what means are used to scan hosts for vulnerabilities. Various ports can be specified as well as the sensor used.

Syntax

```
config vm scan-profile
  edit <scan-profile_str>
    set comment <string>
    set scan-dead-host {enable | disable}
    set sensor <sensor_str>
    set tcp-3way-handshake {enable | disable}
    set tcp-port-adtn <string>
    set tcp-port-grp {full | standard | light | none}
    set udp-port-adtn <string>
    set udp-port-grp {full | standard | light | none}
  end
```

Variables	Description	Default
`<scan-profile_str>`	Enter the name of the scan profile you want to edit. To create a new scan profile, enter a new name.	No default
`comment <string>`	Enter an optional description of the scan profile.	No default
`scan-dead-host {enable | disable}`	Enable to force the FortiAnalyzer unit scan hosts that appear to be unreachable. Some hosts may not return pings although they are still active. Enabling this option will significantly increase the time required to complete a scan.	`disable`
`sensor <sensor_str>`	Enter the name of the sensor this scan profile uses. A sensor is required.	No default
`tcp-3way-handshake {enable | disable}`	Enabled to have the FortiAnalyzer unit establish a connection with the host using the TCP-standard 3-way handshake. Closing the connection is also performed the same way.	`disable`
`tcp-port-adtn <string>`	Enter any ports you want scanned in addition to those specified with the `tcp-port-grp` command. Enter individual ports separating by commas. Enter port ranges, separating the start and end ports with a dash. For example, `set tcp-port-adtn 10,12,14,20-30`	No default
`tcp-port-grp {full | standard | light | none}`	Select the type of TCP port scan the VM scan will execute. • `full` scans all TCP ports. This is the most thorough scan, but it also takes the longest. • `standard` scans about 1800 of the most commonly used TCP ports. • `light` scans about 160 of the most commonly used TCP ports. • `none` disables the TCP port scan.	`none`

Variables	Description	Default
udp-port-adtn <string>	Enter any ports you want scanned in addition to those specified with the udp-port-grp command. Enter individual ports separating by commas. Enter port ranges, separating the start and end ports with a dash. For example, set udp-port-adtn 100,115,200-250,9500	No default
udp-port-grp {full | standard | light | none}	Select the type of UDP port scan the VM scan will execute. • full scans all UDP ports. This is the most thorough scan, but it also takes the longest. • standard scans about 180 of the most commonly used UDP ports. • light scans about 30 of the most commonly used UDP ports. • none disables the UDP port scan.	none

Example

This example details the commands required to make a scan profile called all_tcp-udp. The profile calls the email_only sensor and scans all TCP and UDP ports.

```
config vm scan-profile
  edit all_tcp-udp
    set sensor email_only
    set tcp-port-grp full
    set udp-port-grp full
  end
```

History

4.0	New.

Related commands

- vm sensor

vm schedule

Vulnerability reports are generated based on schedules. Multiple schedules can be created to automatically generate the required reports whenever needed.

Syntax

```
config vm schedule
  edit <schedule_str>
    set asset-group <grp_str>
    set date <date_str>
    set day-of-month <date_int>
    set day-of-week {sun | mon | tue | wed | thu | fri | sat}
    set format {html mht pdf rtf txt}
    set hour <hour_int>
    set max-occurrence <max_int>
    set minute <minute_int>
    set output-profile <profile_str>
    set recurrence {daily | weekly | monthly}
    set scan-profile <profile_str>
    set schedule {run-now | run-later}
  end
```

Variables	Description	Default
`<schedule_str>`	Enter the name of the schedule you want to edit. To create a schedule, enter a new name.	No default
`asset-group <grp_str>`	Enter the asset group on which the network map scan will run.	No default
`date <date_str>`	Enter the date a scheduled scan will start. The date must be formatted as a four digit year, a two digit month, and a two digit day, each separated by a dash. For example, `2009-12-01` would be formatted properly. If left blank, the schedule will start on the current day, subject to the schedule itself.	No default
`day-of-month <date_int>`	Specify the date on which a monthly schedule runs.	No default
`day-of-week {sun | mon | tue | wed | thu | fri | sat}`	Specify the day of the week on which a weekly schedule runs.	No default
`format {html mht pdf rtf txt}`	Enter the required output format or formats of the scan report.	`html`
`hour <hour_int>`	Specify when during the day a scheduled scan will run. Use this command with `minute` to specify an exact time.	`12`
`max-occurrence <max_int>`	Enter the maximum number of times this scheduled scan runs. Enter `0` for no maximum.	`0`
`minute <minute_int>`	Specify when during the day a scheduled scan will run. Use this command with `hour` to specify an exact time.	`0`
`output-profile <profile_str>`	Enter the report output profile name.	No default
`pci-compliance <enable | disable>`	Enable to enforce PCI compliant vulnerability scans. This will have the schedule use the pci_profile regardless of which profile you may have selected.	`disable`
`recurrence {daily | weekly | monthly}`	Enter how often a scheduled scan is run. • `daily` has the FortiAnalyzer run the scan once a day. Use the `hour` and `minute` commands to specify when during the day the scan is run. • `weekly` has the FortiAnalyzer run the scan once a week. Use the `day-of-week`, `hour`, and `minute` commands to specify when during the week the scan is run. • monthly has the FortiAnalyzer run the scan once a month. Use the `day-of-month`, `hour`, and `minute` commands to specify when during the month the scan is run.	`daily`
`scan-profile <profile_str>`	Enter the name of the scan profile to use.	No default
`schedule {run-now | run-later}`	Specify whether the schedule will run once or at regular intervals. • `run-now` will have the FortiAnalyzer run the schedule immediately, and only once. • `run-later` will have the FortiAnalyzer run the schedule at regular intervals, as specified with the `recurrence` command.	`run-now`

Example

This example details the commands required to create a vm scan schedule named `fri-servers`. This schedule will scan the `all-servers` asset-group every Friday at 3:15 A.M. using the `all_tcp-udp` scan profile.

```
config vm schedule
  edit fri-servers
```

```
      set asset-group all-servers
      set schedule run-later
      set recurrence weekly
      set day-of-week fri
      set hour 3
      set minute 15
      set scan-profile all_tcp-udp
    end
```

History

4.0	New.

Related commands

- vm asset-group
- vm scan-profile

vm sensor

Sensors define which vulnerabilities the vulnerability scan checks your hosts for. Create different sensors to specify only the vulnerabilities you need to check for. Sensors can be specified in more than one profile.

Syntax

```
config vm sensor
  edit <sensor_str>
    config filter
      edit <filter_str>
        set authentication {snmp windows unix none}
        set bug {existent | ignore | nonexistent}
        set category {all Applications Backdoor DOS Database Email
           File_Transfer Finger ICMP Instant_Messenger Miscellaneous
           Name_Server NetBIOS Operating_System P2P Policy RPC Remote_access
           SNMP Tools VoIP Web_Applications Web_Client Web_Server Worm}
        set cve {existent | ignore | nonexistent}
        set end-date <string>
        set exposed {yes | no | ignore}
        set ips {existent | ignore | nonexistent}
        set patch {existent | ignore | nonexistent}
        set severity {information low medium high critical}
        set start-date <string>
        set top20 {forti20 sans20}
        set type {include | exclude}
        set vendor {existent | ignore | nonexistent}
      end
    config override
      edit <override_str>
        set type {include | exclude}
        set fid <string>
      end
    set comment <comment_str>
  end
```

Variables	Description	Default
`<sensor_str>`	Enter the name of an existing sensor to edit it, or enter a new name to create a new sensor.	
`<filter_str>`	Enter the name of an existing filter to edit it, or enter a new name to create a new filter.	
`<override_str>`	The name of an override. Enter the name of an existing override to edit it, or enter a new name to create a new override.	
`authentication {snmp windows unix none}`	Scanning for some vulnerabilities requires that the FortiAnalyzer unit authenticate with the hosts to be scanned. Enter the vulnerabilities to include by the authentication they require. Enter the required options, or enter `none` to indicate no authentication.	No default
`bug {existent | ignore | nonexistent}`	Include vulnerabilities depending on whether they've been assigned a Bug Traq ID. • `existent` - restrict the included vulnerabilities to only those with a Bug Traq ID. • `nonexistent` - restrict the included vulnerabilities to only those without a Bug Traq ID. • `ignore` - do not restrict the included vulnerabilities based on whether they have been assigned a Bug Traq ID.	`ignore`
`category {all Applications Backdoor DOS Database Email File_Transfer Finger ICMP Instant_Messenger Miscellaneous Name_Server NetBIOS Operating_System P2P Policy RPC Remote_access SNMP Tools VoIP Web_Applications Web_Client Web_Server Worm}`	Enter a category or categories to limit the vulnerabilities included in the filter. Enter `all` to include all categories, effectively disabling categories as a means of limiting the vulnerabilities included in the filter.	No default
`comment <comment_str>`	Enter an optional description of the sensor.	No default
`cve {existent | ignore | nonexistent}`	Include vulnerabilities depending on whether they've been assigned a CVE ID. • `existent` - restrict the included vulnerabilities to only those with a CVE ID. • `nonexistent` - restrict the included vulnerabilities to only those without a CVE ID. • `ignore` - do not restrict the included vulnerabilities based on whether they have been assigned a CVE ID.	`ignore`
`end-date <string>`	Vulnerabilities include the date they were last modified. No vulnerabilities updated after the entered date will be included in the filter.	No default
`exposed {yes | no | ignore}`	Restrict the vulnerabilities included in the filter based on whether they have been detected in previous scans using this sensor. • `yes` - restrict the included vulnerabilities to only those that have been detected in previous scans using this sensor. • `no` - restrict the included vulnerabilities to only those that have not been detected in previous scans using this sensor. • `ignore` - do not restrict the vulnerabilities included in the filter based on whether they have been detected in previous scans using this sensor.	`ignore`
`fid <string>`	Enter the Fortinet Vulnerability ID. Separate multiple FID numbers with commas.	No default

Variables	Description	Default
`ips {existent | ignore | nonexistent}`	Include vulnerabilities depending on whether they are also FortiGuard IPS signatures. • `existent` - restrict the included vulnerabilities to only those that are FortiGuard IPS signatures. • `nonexistent` - restrict the included vulnerabilities to only those that are not FortiGuard IPS signatures. • `ignore` - do not restrict the included vulnerabilities based on whether they are FortiGuard IPS signatures.	`ignore`
`patch {existent | ignore | nonexistent}`	Include vulnerabilities depending on whether a patch exists to fix them. • `existent` - restrict the included vulnerabilities to only those with a patch. • `nonexistent` - restrict the included vulnerabilities to only those without a patch. • `ignore` - do not restrict the included vulnerabilities based on whether they have a patch.	`ignore`
`severity {information low medium high critical}`	All vulnerabilities are assigned a relative severity level. Enter the severity levels to include in the filter. Enter all five severity levels to effectively disable severity as a means of limiting the vulnerabilities included in the filter.	No default
`start-date <string>`	Vulnerabilities include the date they were last modified. No vulnerabilities updated before the entered date will be included in the filter.	No default
`top20 {forti20 sans20}`	Specify one or both of these top 20 vulnerability lists to restrict included vulnerabilities to those also on the list you specify.	No default
`type {include | exclude}`	Specify whether the vulnerability attributes you select when creating a filter will define the vulnerabilities that are included, or the vulnerabilities that are excluded.	`include`
`vendor {existent | ignore | nonexistent}`	Include vulnerabilities depending on whether they include a link to the vendor description of the problem. This link appears in the *Vendor Reference* column of the vulnerability database. • `existent` - restrict the included vulnerabilities to only those with a link. • `nonexistent` - restrict the included vulnerabilities to only those without a link. • `ignore` - do not restrict the included vulnerabilities based on whether they have a vendor reference link.	`ignore`

Example

This example details the commands required to make a VM sensor called `email_only`. The sensor contains a filter named `email_filter` that includes all signatures with three matching characteristics:

- The signatures detect email vulnerabilities.
- The signatures have a severity rating of high or critical.
- The vulnerabilities have patches.

```
config vm sensor
  edit email_only
    config email_filter
      edit filter_name
        set category email
        set severity high critical
        set patch existent
      end
  end
```

History

4.0 New.

Related commands

- vm scan-profile

execute

The `execute` commands perform immediate operations on the FortiAnalyzer unit. This command can:

- back up and restore the system configuration, log files, HTTPS certificates, or reset the unit to default settings
- set the unit date and time
- diagnose network problems by using `ping`
- import logs that have been backed up
- update vulnerability management services.

When ADOMs are enabled, there are only four `execute` commands available within each ADOM, including the root ADOM. These four execute commands are:

- `column-settings`
- `content-files`
- `quarantine_files`
- `ips-pkt`

This chapter contains the following sections:

admin-cert

Use this command to change a HTTPS certificate to a new certificate signed by a regular Certificate Authority instead of Fortinet.

Syntax

```
execute admin-cert import
{<service[ftp|sftp|scp|tftp]>|<ip_address>|<argument_1>|
<argument_2>|<argument_3>}
execute admin-cert reset
execute admin-cert show
```

Keywords and variables	Description
`import {<service[ftp|sftp|scp|tftp]>|<ip_address>|<argument_1>|<argument_2>|<argument_3>}`	Imports the server certificate (PKCS12 format) from a specified server. The following explains the variables referred to as “argument_<number>”. • `<argument_1>` – For FTP, SFTP or SCP, enter a user name. For TFTP, enter a directory or filename. • `<argument_2>` – For FTP, SFTP or SCP, enter a password or “-”. For TFTP, enter a filename or PKCS12 file password or “-”. • `<argument_3>` – For FTP, SFTP or SCP, enter a directory or filename. For TFTP, enter a PKCS12 file password or “-”.
`reset`	Resets the server certificate information.
`show`	Displays the information about the current certificate.

Examples

The following example shows what displays when you enter the command syntax `execute admin-cert show`:

```
    Subject:
             C = US
             ST = CA
             L = Santa Clara
             O = “Fortinet, Inc.”
             CN = Fortinet
             emailAddress = support@fortinet.com
    Issuer:
            C = US
            ST = CA
            L = Sanata Clara
            O = “Fortinet, Inc.”
            CN = Fortinet
            emailAddress = support@fortinet.com
    Valid from:
                2009-01-07 13:08:31 GMT
    Valid to:
                2019-01-12 13:08:31 GMT

  Version:

            3

  SN:

            0
```

History

3.0 MR7	New command.
4.0 MR1	Added `import` and `reset` keywords. Removed `self-sign` keyword.

backup

Use this command to back up the FortiAnalyzer configuration, device log or report files to a server.

Syntax

```
execute backup config {[ftp | sftp | scp | tftp] <ip_address> <arg_1> <arg_2>
<arg_3> <arg_4>}
execute backup config-secure {[ftp | sftp | scp | tftp] <ip_address> <arg_1>
<arg_2> <arg_3> <arg_4>}
execute backup ediscovery {all | <folder_name>} {ftp | scp | sftp | tftp}
<server_ipv4> <username_str> <password_str> <directory_str> <file_name>
execute backup logs {[all | <devices_str>] [ftp | scp | sftp | tftp]
<server_ipv4> <username_str> <password_str> <directory_str>}
execute backup logs-only {[ftp | sftp | scp | tftp] <ip_address> <arg_1>
<arg_2> <arg_3> <arg_4>}
execute backup reports {all | <devices_str>} {ftp | scp | sftp | tftp}
<server_ipv4> <username_str> <password_str> <directory_str>
```

Keywords and variables	Description
`config {[ftp | sftp | scp | tftp] <ip_address> <arg_1> <arg_2> <arg_3> <arg_4>}`	Back up the system configuration to a file on a FTP, SFTP, SCP, or TFTP server. • `arg_1` – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename. • `arg_2` – For FTP, SFTP or SCP enter a password or enter '-'. For TFTP enter the filename or press Enter. • `arg_3` – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter. • `arg_4` – Enter a filename or press Enter. **Note:** Use the FTP server's IP address whenever you are entering the FTP server information. Using a domain name is not supported.
`config-secure {[ftp | sftp | scp | tftp] <ip_address> <arg_1> <arg_2> <arg_3> <arg_4>}`	Back up an encrypted system configuration file to a FTP, SFTP, SCP, or TFTP server. • `arg_1` – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename. • `arg_2` – For FTP, SFTP or SCP enter a password or enter '-'. For TFTP enter the filename or press Enter. • `arg_3` – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter. • `arg_4` – Enter a filename or press Enter. **Note:** Use the FTP server's IP address whenever you are entering the FTP server information. Using a domain name is not supported.
`ediscovery {all | <folder_name>} {ftp | scp | sftp | tftp} <server_ipv4> <username_str> <password_str> <directory_str> <file_name>`	Back up the eDiscovery files to a FTP, SFTP, SCP, or TFTP server. • `arg_1` – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename. • `arg_2` – For FTP, SFTP or SCP enter a password or enter '-'. For TFTP enter the filename or press Enter. • `arg_3` – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter. • `arg_4` – Enter a filename or press Enter. **Note:** Use the FTP server's IP address whenever you are entering the FTP server information. Using a domain name is not supported.

Keywords and variables	Description
`logs {[all | <devices_str>] [ftp | scp | sftp | tftp] <server_ipv4> <username_str> <password_str> <directory_str>}`	Back up device log file, content archives and quarantines to an FTP, SCP (SSH), SFTP, or TFTPserver. `<devices_str>` indicates the devices to which the log files belong. It can be a single device name, a comma-separated list of device names, or `all` for all devices. `<directory_str>` is optional. If it is not specified, then the FortiAnalyzer unit creates a directory named `backup_logs` on the server. If you select the protocol `tftp`, do not enter `<username_str>`; `<password_str>` is optional. **Note:** Use the FTP server's IP address whenever you are entering the FTP server information. Using a domain name is not supported.
`logs-only {[ftp | sftp | scp | tftp] <ip_address> <arg_1> <arg_2> <arg_3> <arg_4>}`	Back up only logs from the specified device. **Note:** Use the FTP server's IP address whenever entering the FTP server information. Using a domain name is not supported.
`reports {all | <devices_str>} {ftp | scp | sftp | tftp} <server_ipv4> <username_str> <password_str> <directory_str>`	Back up device report file(s) to an FTP, SCP (SSH), SFTP, or TFTP server. `<devices_str>` indicates the devices to which the log files belong. It can be a single device name, a comma-separated list of device names, or `all` for all devices. `<directory_str>` is optional. If it is not specified, then the FortiAnalyzer unit creates a directory named `backup_logs` on the server. If you select the protocol `tftp`, do not enter `<username_str>`; `<password_str>` is optional. Only completed reports will be backed up. Reports which are being generated or have not yet started when this command is executed will not be backed up. **Note:** Use the FTP server's IP address whenever you are entering the FTP server information. Using a domain name is not supported.

Examples

The following backs up a FortiAnalyzer-800 system configuration to a file named `fa800.cfg` to a TFTP server at IP address 192.168.1.23.

```
execute backup config tftp fa800.cfg 192.168.1.23 ******
```

The following backs up log files for a device named `FG50B12205400050` to an FTP server at IP address 192.168.1.24.

```
execute backup logs FG50B12205400050 ftp 192.168.1.24 user1 p8ssw0rd
   ftpbackup/FGT50B/
```

A confirmation message appears:

```
Note: This command is designed to backup all logs to a specified server
      prior to changing RAID level and/or formatting the disks.
      Executing it frequently is not recommended!
Do you want to continue? (y/n)y
```

If you select to continue by entering 'y,' status messages appear, similar to the following:

```
Preparing for FG50B12205400050
    log files...
    email dlp archived files...
    http dlp archived files...
    ftp dlp archived files...
    im dlp archived files...
    mms dlp archived files...
```

```
      quarantined files...
Backing up FG50B12205400050 ...
Backup has been finished successfully.
```

History

3.0 MR1	Added `logs`. This replaces the command backup_restore_logs.
3.0 MR5	New command `execute backup restore`. Backs up reports to an FTP or TFTP server.
3.0 MR6	New options `sftp` and `scp` for `execute backup logs` and `execute backup reports`. Select SFTP and SCP protocols for log or report backup.
3.0 MR7	Added new keyword, `https-cert`.
4.0	New keywords were added: • `<arg_1>` • `<arg_2>` • `<arg_3>` • `<arg_4>` The command, `config-secure`, was also added in this release.
4.0 MR1	Removed `https-cert` keyword.

column-settings

Use this command to change column settings for administrators. When ADOMs are enabled, this command is not available within the global command; however, it is available within each ADOM and the root ADOM.

Syntax

```
execute column-settings clone <from_administrator>
execute column-settings reset <administrator_name>
```

Keywords and variables	Description
`clone <from_administrator>`	Enter an administrator name to duplicate those same settings for another administrator. For example, you want to clone admin_1 settings to admin_2 settings, so you enter admin_1.
`reset <administrator_name>`	Enter one administrator name or multiple administrator names to reset their column settings to default.

Examples

The following example shows how to clone settings from the administrator admin_headquarters to admin_branchoffice.

```
execute column-settings clone admin_headquarters
```

History

4.0	New.

disconnect

Use this command to disconnect an administrator from the FortiAnalyzer unit by logging them out of the system.

Syntax

```
execute disconnect <administratorlogin_id>
```

Keywords and variables	Description
`disconnect <administratorlogin_id>`	Enter the administrator login ID, which is found in the Index column. By entering the command followed by a question mark (?), you can view all currently connected administrative users.

Example

In this example, the following determines who is logged in by entering:

```
execute disconnect ?
```

A list of currently logged-in administrators appears:

```
Index    Login name       Login type      Login from
 0        admin            CLI             ssh (10.10.20.154)
 1        admin            WEB             10.20.10.15
```

The command syntax to log out the administrator that is logged in to the web-based manager is:

```
execute disconnect 1
```

dlp-files

Use this command to delete files from the DLP archived log files. This command only deletes archived files, not the metadata information. To delete the metadata information, use the `execute dlp-summaries` command.

When ADOMs are enabled, this command is not available within the global command; however, it is available within each ADOM and the root ADOM.

Syntax

```
execute dlp-files clear {all | email | im | ftp | http | mms} <device_str>
```

Keywords and variables	Description
`clear {all	email	im	ftp	http	mms} <device_str>`	Delete the DLP files for the specified device and protocol from the DLP archived logs.

Example

You could clear all archived email messages for a device named `fgt-50B`.

```
execute dlp-files clear email fgt-50B
```

History

3.0 MR4	New command.
3.0 MR5	Added `mms` option.
4.0 MR1	Renamed `content-files` to `dlp-files`.

dlp-summaries

Use this command to delete a device’s metadata information and archived files from the DLP archived log files.

When ADOMs are enabled, this command is not available within the global command; however, it is available within each ADOM and the root ADOM.

Syntax

```
execute dlp-summaries clear {all | email | im | ftp | http | mms} <device_str>
```

Keywords and variables	Description
`clear <device_str>`	Delete the DLP information, including the metadata and files for the specified device from the DLP archived logs.

History

4.0 MR2	New.

factoryreset

Caution: This procedure deletes all changes that you have made to the FortiAnalyzer configuration and reverts the system to the installed firmware version’s default configuration, including resetting interface addresses.

Use this command to reset the FortiAnalyzer configuration to the firmware’s default settings.

Syntax

```
execute factoryreset
```

formatlogdisk

Caution: This operation will erase all data on the hard disk, including quarantine and log files.

Use this command to format the FortiAnalyzer hard disk to enhance performance for logging.

Syntax

```
execute formatlogdisk
```

import logs

Use this command to import logs from a specific device or from FortiClient.

Syntax

```
execute import logs [<device_1> | <device_2> | <device_3>…]
execute import logs from-file [ftp | sftp | scp | tftp]
execute import logs All_FortiClients
```

Keywords and variables	Description
`[<device_1>	<device_2>	<device_3>…]`	Enter the device you want to import logs from.
`from-file [ftp	sftp	scp	tftp]`	Enter to use the device_id in the imported files.
`All_FortiClients`	Enter to import all FortiClient logs.

Examples

The following shows how to import logs from a device.

```
execute import logs FGT_50B
```

History

4.0	Revised. Updates the `importlog` command.

import-lang

Use this command to import a customized report language file.

Syntax

```
execute import-lang <language_name> <tftp_ip_address> <language_format_name>
<language_string_name> <language_font_name>
```

Keyword	Description
`<language_name>`	Enter the name of the language format file located in the TFTP server's root directory.
`<tftp_ip_address>`	Enter the TFTP server's IP address.
`<language_format_name>`	Enter the name of the language format file located in the TFTP server's root directory.
`<language_string_name>`	Enter the name of the language string file located in the TFTP server's root directory.
`<language_font_name>`	Enter the name of the language font file located in the TFTP server's root directory. This is optional.

Example

You could create a report language customization named `English_Custom`.

```
execute importlog English_Custom 192.168.1.23 English_Custom.format
    English_Custom.string myfont.ttf
```

History

3.0 MR6 New command `execute import-lang`. Uploads report language customization files from a TFTP server.

ips-pkt

Use this command to delete files from a specified device. When ADOMs are enabled, this command is not available within the global command; however, it is available within each ADOM and the root ADOM.

Syntax

```
execute ips-pkt clear <device_name>
```

Keywords and variables	Description
`clear <device_name>`	Enter to delete files from a specific device.

History

4.0 New.

log-integrity

Use this command to query a log file's MD5 checksum and timestamp to ensure its integrity and validity . This command only applies for:

- rolled log files with MD5 hash recorded.
- a local log containing the MD5 hash of the log files downloaded from the Fortinet web-based manager.

Active log file cannot be checked with this command.

Keywords and variables	Description
`log-integrity <device_name> <log_file_name>`	Enter a device’s log file name to query the file's MD5 checksum and timestamp.

Example

You can query the checksum and timestamp of a log file as following:

```
execute log-integrity FG500A0000000005 tlog.1283185861.log
MD5 checksum: f33ad90feb46351434a1a60565901780, checksum timestamp:
   1283185904 (Mon Aug 30 17:31:44 2010)
```

History

4.3 New.

migration

Use this command to abort, pause or test the migration.

Syntax

```
execute migration {cancel | pause | resume | start | test}
```

Keywords and variables	Description
`{cancel	pause	resume	start	test}`	Enter to cancel, pause, resume, start, or test the migration.

History

4.0 MR1 New.

ping

Use this command to send an ICMP echo request (ping) to test the network connection between the FortiAnalyzer unit and another network device.

Syntax

```
execute ping <address_ipv4>
```

Example

You could ping a host with the IP address 192.168.1.23.

```
   execute ping 192.168.1.23
```

ping-options

Use this command to set ICMP echo request (ping) options to control the way ping tests the network connection between the FortiAnalyzer unit and another network device.

Syntax

```
execute ping-options data-size <bytes>
execute ping-options df-bit {yes | no}
execute ping-options pattern <2-byte_hex>
execute ping-options repeat-count <repeats_int>
execute ping-options source {auto | <source-intf_ip>}
execute ping-options timeout <seconds_int>
execute ping-options tos <service_type_int>
execute ping-options ttl <hops_int>
execute ping-options validate-reply {yes | no}
execute ping-options view-settings
```

Keyword	Description	Default
`data-size <bytes>`	Specify the datagram size in bytes.	56
`df-bit {yes	no}`	Set `df-bit` to `yes` to prevent the ICMP packet from being fragmented. Set `df-bit` to `no` to allow the ICMP packet to be fragmented.	no
`pattern <2-byte_hex>`	Used to fill in the optional data buffer at the end of the ICMP packet. The size of the buffer is specified using the `data_size` parameter. This allows you to send out packets of different sizes for testing the effect of packet size on the connection.	No default.

Keyword	Description	Default
`repeat-count <repeats_int>`	Specify how many times to repeat ping.	`5`
`source {auto | <source-intf_ip>}`	Specify the FortiAnalyzer interface from which to send the ping. If you specify `auto`, the FortiAnalyzer unit selects the source address and interface based on the route to the `<host-name_str>` or `<host_ip>`. Specifying the IP address of a FortiAnalyzer interface tests connections to different network segments from the specified interface.	`auto`
`timeout <seconds_int>`	Specify, in seconds, how long to wait until ping times out.	`2`
`tos <service_type_int>`	Set the ToS (Type of Service) field in the packet header to provide an indication of the quality of service wanted. • lowdelay = minimize delay • throughput = maximize throughput • reliability = maximize reliability • lowcost = minimize cost • default = 0	`default/0`
`ttl <hops_int>`	Specify the time to live. Time to live is the number of hops the ping packet should be allowed to make before being discarded or returned.	`64`
`validate-reply {yes | no}`	Select `yes` to validate reply data.	`no`
`view-settings`	Display the current ping-option settings.	No default.

Example

Use the following command to increase the number of pings sent.

```
execute ping-options repeat-count 10
```

Use the following command to send all pings from the FortiAnalyzer interface with IP address 192.168.10.23.

```
execute ping-options source 192.168.10.23
```

quarantine-files

Use this command to delete the quarantine files for a FortiGate unit. When ADOMs are enabled, this command is not available within the global command; however, it is available within each ADOM and the root ADOM.

Syntax

```
execute quarantine-files clear <device_str>
```

Example

You could delete quarantines files from the FortiAnalyzer unit for a FortiGate named `fgt-50B`.

```
execute quarantine-files clear fgt-50B
```

History

3.0 MR4	New command.

reboot

Use this command to restart the FortiAnalyzer unit.

Syntax

```
execute reboot
```

reload

Use this command to reload the FortiAnalyzer unit configuration.

Syntax

```
execute reload
```

History

3.0 MR1	New command added.

reset-sqllog-transfer

Use this command to send logs received by the FortiAnalyzer unit to the SQL database for generating reports.

The FortiAnalyzer unit supports both local and remote SQL database options. The advantages of using the SQL database are:

- Flexibility: Through the use of standard SQL queries, more flexible reporting capabilities can be offered.
- Scalability: Through the use of a remote SQL database, any upper bound on the amount of available log storage is removed. Furthermore, the hardware of an external SQL database server can be more easily upgraded to support growing performance needs.

Syntax

```
execute reset-sqllog-transfer
```

History

4.0 MR2	New.

restore

Use this command to:

- restore configuration backups
- change the FortiAnalyzer firmware
- restore device log or report backups to the FortiAnalyzer unit

Syntax

```
execute restore config {[ftp | sftp | scp | tftp] <ip_address> <arg_1> <arg_2>
<arg_3> <arg_4>}
execute restore config-secure {[ftp | sftp | scp | tftp] <ip_address> <arg_1>
<arg_2> <arg_3> <arg_4>}
execute restore image {[ftp | sftp | scp | tftp] <ip_address> <arg_1> <arg_2>
<arg_3> <arg_4>}
execute restore logs {[all | All_FortiClients | <device_name(s)] [ftp | sftp |
scp] <ip_address> <user_name> <password> <directory_str>
execute restore logs-only {[all | All_FortiClients | <device_name(s)>][ftp |
sftp | scp] <ip_address> <user_name> <password> <directory>}
execute restore reports {[all | <report_name(s) | <report_name_pattern>] [ftp
| sftp | scp] <user_name> <password> <directory>
execute restore vm {[ftp | sftp | scp |tftp]> <ip_address> <arg_1> <arg_2>
<arg_3> arg_4>}
```

Variables	Description
`image {[ftp	sftp	scp	tftp] <ip_address> <arg_1> <arg_2> <arg_3> <arg_4>}`	Upload a firmware image from a TFTP server to the FortiAnalyzer unit. The FortiAnalyzer unit reboots, loading the new firmware. • `arg_1` – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename. • `arg_2` – For FTP, SFTP or SCP enter a password or enter ‘-’. For TFTP enter the filename or press Enter. • `arg_3` – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter. • `arg_4` – Enter a filename or press Enter.
`config {[ftp	sftp	scp	tftp] <ip_address> <arg_1> <arg_2> <arg_3> <arg_4>}`	Restore the system configuration from a backup file on a TFTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords. • `arg_1` – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory. • `arg_2` – For FTP, SFTP or SCP enter a password or enter ‘-’. For TFTP enter the filename. • `arg_3` – For FTP, SFTP or SCP enter a directory. For TFTP, press Enter. • `arg_4` – Enter a filename and press Enter.
`config-secure {[ftp	sftp	scp	tftp] <ip_address> <arg_1> <arg_2> <arg_3> <arg_4>}`	Restore the encrypted configuration file. • `arg_1` – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename. • `arg_2` – For FTP, SFTP or SCP enter a password or enter ‘-’. For TFTP enter the filename or press Enter. • `arg_3` – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter. • `arg_4` – Enter a filename or press Enter.
`logs {[all	All_FortiClients	<device_name(s)] [ftp	sftp	scp] <ip_address> <user_name> <password> <directory_str>`	Restore log files and DLP archives to the FortiAnalyzer hard disk. • `device_name(s)` – Separate multiple device names with a comma. If you want to restore all log files, use the keyword, `all`.
`logs-only {[all	All_FortiClients	<device_name(s)>][ftp	sftp	scp] <ip_address> <user_name> <password> <directory>}`	Restore device logs from a specific device. • `All_FortiClients` – This will restore all log files that were recorded by FortiClients. • `device_name(s)` – Multiple device names need to be separated by a comma. If you want to restore all log files, use the `all` keyword.

Variables	Description
`reports {[all | <report_name(s) | <report_name_pattern>] [ftp | sftp | scp] <user_name> <password> <directory>`	Restore device report files to the FortiAnalyzer hard disk. • `report_name(s)` – Multiple report names need to be separated by a comma; if you want to restore all reports use the keyword `all`. • `report_name_pattern` – Use this keyword when you want to specify group of reports that contain a certain pattern. For example, you enter foo* all reports starting with the letters foo will be restored.
`https-cert {[ftp | sftp | scp | tftp] <ip_address> <arg_1> <arg_2> <arg_3> <arg_4>}`	Restore the HTTPS certificate and private key. The file that you are restoring must be in the format, PKCS12; no other format is accepted. • `arg_1` – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory. • `arg_2` – For FTP, SFTP or SCP enter a password or enter '-'. For TFTP enter the filename. • `arg_3` – For FTP, SFTP or SCP enter a directory or filename. For TFTP, enter a PKCS12 file password or '-'. • `arg_4` – For FTP, SFTP or SCP enter a file name or PKCS12 file password, or '-'. For TFTP, press Enter.
`vm {[ftp | sftp | scp |tftp]> <ip_address> <arg_1> <arg_2> <arg_3> arg_4>}`	Restore vulnerabilities from an FTP, SFTP, SCP or TFTP server. • `arg_1` – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename. • `arg_2` – For FTP, SFTP or SCP enter a password or enter '-'. For TFTP enter the filename or press Enter. • `arg_3` – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter. • `arg_4` – Enter a filename or press Enter.

Example

The following example uploads a configuration file from a TFTP server to the FortiAnalyzer unit and restarts the FortiAnalyzer unit with this configuration. The name of the configuration file on the TFTP server is `backupconfig.cfg`. The IP address of the TFTP server is 192.168.1.23.

```
execute restore config tftp 192.168.1.23 backupconfig.cfg
```

This example restores device log files for a FortiGate-50B named `FGT50B02803033050`.

```
execute restore logs FGT50B2803033050 tftp 192.168.1.24 admin1 p8sswOrd
   d:\FGT50B
```

A confirmation message appears:

```
Note: This command restores all logs from a specified server which were
   backed up prior to changing the RAID level or formatting the disks.
   Executing it frequently is not recommended!
Do you want to continue? (y/n)y
```

A second confirmation message appears:

```
The restore operation will overwrite any logs already on the FortiAnalyzer
   for this device.
Do you want to continue? (y/n)y
```

If you select to continue by entering 'y,' the following status messages appear:

```
Restoring device FGT50B2803033050 ...
Restore has been finished successfully.
System is rebooting...
```

When following the restoration of a log file or files, you will need to reconnect to the CLI.

History

3.0 MR1	Added `logs`. This replaces the command `backup_restore_logs`.
3.0 MR5	New command `execute restore reports`. Restores report backup from an FTP server.
3.0 MR7	Added new keyword, `https-cert`.
4.0	New keywords were added: • `<arg_1>` • `<arg_2>` • `<arg_3>` • `<arg_4>` The commands, `config-secure` and `vm` were also added in this release.
4.0 MR1	Removed the `https-cert` keyword .

run

Syntax

```
execute run prog [arg...]
```

Keywords and variables	Description
`prog [arg...]`	

History

4.0 MR2	New.

set-date

Use this command to set the system date.

Syntax

```
execute set-date <date_str>
    date_str has the form mm/dd/yyyy, where
```

- `mm` is the month and can be `01` to `12`
- `dd` is the day of the month and can be `01` to `31`
- `yyyy` is the year and can be `2001` to `2037`

If you do not specify a date, the command returns the current system date.

Example

This example sets the date to 17 March 2009:

```
    execute set-date 17/03/2009
```

set-time

Set the system time.

Syntax

```
execute set-time <time_str>
    time_str has the form hh:mm:ss, where
```

- `hh` is the hour and can be `00` to `23`
- `mm` is the minutes and can be `00` to `59`
- `ss` is the seconds and can be `00` to `59`

If you do not specify a time, the command returns the current system time.

Example

This example sets the system time to 15:31:03:

```
    execute set-time 15:31:03
```

shutdown

Use this command to shut down the FortiAnalyzer unit.

Syntax

```
execute shutdown
```

sql-local

Use this command to remove logs from the local SQL database.

Syntax

```
execute sql-local {remove-db | remove-device <device_ID> | remove-logtype
<log_type>}
```

Keywords and variables	Description
`remove-db`	Delete all logs saved in the local SQL database.
`remove-device <device_ID>`	Delete all logs of the selected device from the local SQL database.
`remove-logtype <log_type>`	Delete all logs of the selected type from the local SQL database.

Example

This example removes all logs of device `FG5A253E07600124` from the local SQL database:

```
execute sql-local remove-device FG5A253E07600124
```

History

4.0 MR2	New.

sql-query-dataset

Use this command to test the SQL dataset query.

Syntax

```
execute sql-query-dataset <dataset_name> <device/group_name> <vdom>
```

Keywords and variables	Description
`<dataset_name>`	Select one of the existing datatset.
`<device/group_name>`	Select one of the devices or device groups.
`<vdom>`	Select the VDom of the device, if applicable.

History

4.0 MR2 New.

sql-query-generic

Use this command to run an SQL statement.

Syntax

```
execute sql-query-generic <sql_statement>
```

Keywords and variables	Description
`<sql_statement>`	Enter the SQL statement to run.

History

4.0 MR2 New.

traceroute

Use this command to show a list of routers taken to reach a network IP address or domain name.

Syntax

```
execute traceroute <address_ipv4>
```

History

3.0 MR3 New command.

update-vm

Use this command to immediately update vulnerabilities.

Syntax

```
execute update-vm
```

History

4.0	New.

vm

Use this command to schedule, view vulnerability reports, import hosts, and update vulnerabilities.

Syntax

```
execute vm import-hosts <report_name> <group_name> <force>
execute vm map-config-run <map-config-name>
execute vm map-config-stop <map-config-name>
execute vm report-clear <report-type [scan | map]>
execute vm report-delete <report-type [scan <reportname> | map <reportname> ]
execute vm report-list <report-type [scan | map]> <type> [name| starttime |
endtime]
execute vm schedule-run <schedule_name>
execute vm schedule-stop <schedule_name>
```

Keywords and variables	Description
`import-hosts <report_name> <group_name> <force>`	Enter to import the hosts from a map report.
`map-config-run <map-config-name>`	Enter to run a map configuration only one time.
`map-config-stop <map-config-name>`	Enter to stop a running map configuration.
`report-clear <report-type [scan | map]>`	Enter to clear all scan or map reports.
`report-delete <report-type [scan <reportname> | map <reportname> ]`	Enter to delete one report at a time.
`report-list <report-type [scan | map]> <type> [name| starttime | endtime]`	Enter to list all reports.
`schedule-run <schedule_name>`	Enter to run a schedule one time.
`schedule-stop <schedule_name>`	Enter to stop a running schedule.

Example

The following example shows how to schedule when updates for vulnerabilities should occur.

```
execute vm schedule-run schedule_1
```

History

4.0	New.
4.0 MR1	Removed the following keywords: • `update-fds` • `update-manual` • `update-status-list` • `update-refresh`

get

`get` commands display a part of your FortiAnalyzer 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:

```
FortiAnalyzer# get system dns

primary             : 172.16.95.19
secondary           : 0.0.0.0
```

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:

```
FortiAnalyzer# get system dns
```

and this command would not:

```
FortiAnalyzer# get
FortiAnalyzer(dns)# get system dns
```

FortiAnalyzerMost `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 chapters in this guide.

Other `get` commands, such as `get system performance`, are used to display system information that is ***not*** configurable. This chapter describes this type of `get` command.

This chapter describes the following commands.

get system performance

get system status

Note: Although not explicitly shown in this section, for all `config` commands, there are related `get` and show 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.

system performance

Displays the FortiAnalyzer unit's CPU status, CPU usage, memory usage, and up time.

Syntax

```
get system performance
```

Example

```
FortiAnalyzer# get system performance
CPU states:    0% used, 100% idle
CPU Usage:      %user   %nice   %sys    %idle   %iowait %irq    %softirq
                0.05    44.36   1.40    54.25   0.00    0.00    0.00
```

```
Memory states: 10% used
Uptime:        1 days, 0 hours, 38 minutesCPU usage:     0% used, 100% idle
```

History

v4.0 MR2	New.

Related topics

- get system status

system status

Use this command to display FortiAnalyzer system status information including:

- firmware version, build number and date
- branching point (same as firmware build number)
- release version
- FortiAnalyzer unit serial number and BIOS version
- vulnerability management engine and plugin version
- number of registered host asset IP addresses
- maximum number of host asset IP addresses allowed
- administrative domain status
- maximum number of administrative domains supported
- number of registered devices
- maximum supported devices
- hostname
- FIPS mode status
- system time:

Syntax

```
get system status
```

Example

```
FortiMail-400 # get system status
Version: FortiAnalyzer-800B v4.0,build0172,100120 (Interim)
Branch point: 172
Release Version Information: Interim
Serial-Number: FL800B3908000420
BIOS version: 04000002
VM Engine Version: 1.042 [Mon Nov  9 21:20:00 2009]
VM Plugin Version: 1.086 [Mon Nov  9 21:20:00 2009]
Registered Host Asset IP Addresses: 1
Max Number of Host Asset IP Addresses: 200
Admin Domain Status: disabled
Max number of administrative domains: 50
Registered Devices: 13
Maximum Supported Devices: 500
Hostname: FortiAnalyzer-800B
FIPS mode: disabled
System Time: Fri Jan 22 14:37:47 EST 2010
```

History

v4.0	New.

Related topics

- get system performance

diagnose

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

This chapter contains the following sections:

adom

Use this command to view FortiAnalyzer administrative domain information. You must first add administrative domains before using this command. For more information, see "system global" on page 100.

Syntax

```
diagnose adom {admin <adom> | device <adom> | logfile <adom> |
    report_schedule <adom> | summary <adom>}
```

Variable	Description
`admin <adom>`	Display the administrator name in an ADOM and his/her access profile name. If you do not enter the ADOM name, all FortiAnalyzer administrators and the names of their access profiles appear.
`device <adom>`	Display an ADOM's devices information including the device names, IDs, and disk space used by data from each device. If you do not enter the ADOM name, the information of all devices monitored by the FortiAnalyzer unit appear.
`logfile <adom>`	Display the total number and size of log files in an ADOM. If you do not enter the ADOM name, the total number and size of log files in a FortiAnalyzer unit appear.
`report_schedule <adom>`	Display the names, layouts, number of charts included in each report, devices or device groups associated with the report, and schedules of each report in the ADOM. If you do not enter the ADOM name, all report information on a FortiAnalyzer unit appears.
`summary <adom>`	Display the summary information of the above commands.

Example

This example shows how to display the administrator name in an ADOM and his/her access profile name:

```
diagnose adom admin adom1
```

History

4.0 MR2	New.

alertd

Use this command to manage alert daemon error messages and view its status.

Syntax

```
diagnose alertd error-msg {clear | show | upload <ftp_host_IP>}
diagnose alertd status
```

Variable	Description
`error-msg {clear	show	upload <ftp_host_IP>}`	`clear`: Remove the alert daemon error messages. `show`: Display recent alert daemon error messages. `upload`: Save the alert daemon error messages to an FTP server.
`status`	Display the running status of the alert daemon.

Example

This example shows how to display the alert daemon running status:

```
diagnose alertd status
```

Output:

```
Alert name:alert-event1
Alert Severity: High
More than 1 event(s) occur in last 0.5 hour(s)!
```

History

4.0 MR2	New.

alertmail

Use this command to manage alert mail daemon error messages.

Syntax

```
diagnose alertmail error-msg {clear | show | upload <ftp_host_IP>}
```

Variable	Description
`error-msg {clear	show	upload <ftp_host_IP>}`	`clear`: Remove the alert mail daemon error messages. `show`: Display recent alert mail daemon error messages. `upload`: Save the alert mail daemon error messages to an FTP server.

Example

This example shows how to display the recent alert email daemon error messages:

```
diagnose alertmail error-msg show
```

Output:

```
[2010-01-12 16:14:08] ERROR: alertmail(452):mail_request.c:781:
   _init_mail_info failed: no user
```

History

4.0 MR2	New.

cmdb

Use this command to view Configuration Management Database (CMDB) information and manage CMDB error messages.

Syntax

```
diagnose cmdb cmdb-profile {info | node <path.object[.attribute]>}
diagnose cmdb error-msg {clear | show | upload <ftp_host_IP>}
```

Variable	Description
`cmdb-profile {info	node <path.object[.attribute]>}`	Display CMDB profile share memory information, or CMDB profile by node.
`error-msg {clear	show	upload <ftp_host_IP>}`	`clear`: Removes alert CMDB error messages. `show`: Displays recent CMDB error messages. `upload`: Save the CMDB error messages to an FTP server.

Example

This example shows how to upload the CMDB error messages to an FTP server:

```
diagnose cmdb erro-msg upload 192.168.10.1
```

History

4.0 MR2	New.

debug application

Use this command to set the debug levels for the FortiAnalyzer applications.

Syntax

```
diagnose debug application alert <debug_level_integer>
diagnose debug application alertmail <debug_level_integer>
diagnose debug application cached <debug_level_integer>
diagnose debug application cmdb <debug_level_integer>
diagnose debug application fnbamd <debug_level_integer>
diagnose debug application fortiguard <debug_level_integer>
diagnose debug application fortilogd <debug_level_integer>
diagnose debug application ipsecd <debug_level_integer>
diagnose debug application log-aggregate <debug_level_integer>
diagnose debug application log-indexer <debug_level_integer>
diagnose debug application logfiled <debug_level_integer>
diagnose debug application miglogd <debug_level_integer>
diagnose debug application network-summary <debug_level_integer>
diagnose debug application ntpd <debug_level_integer>
diagnose debug application oftpd <debug_level_integer>
diagnose debug application remote-auth <debug_level_integer>
diagnose debug application report <debug_level_integer>
diagnose debug application samba-nfs <debug_level_integer>
diagnose debug application snmpd <debug_level_integer>
diagnose debug application sql-integration <debug_level_integer>
diagnose debug application sqlplugind <debug_level_integer>
diagnose debug application sumreportsd <debug_level_integer>
diagnose debug application uploadd <debug_level_integer>
diagnose debug application vm <debug_level_integer>}
```

Variable	Description	Default
`alert <debug_level_integer>`	Set the debug level of alert daemon from 0-8. Higher debug level, that is, a bigger number, will display more debug messages.	0
`alertmail <debug_level_integer>`	Set the debug level of alert email daemon from 0-8.	0
`cached <debug_level_integer>`	Set the debug level of CMDB cache daemon from 0-8.	0
`cmdb <debug_level_integer>`	Set the debug level of FortiAnalyzer Web Services from 0-8.	0
`fnbamd <debug_level_integer>`	Set the debug level of the Fortinet authentication daemon from 0-8.	0
`fortiguard <debug_level_integer>`	Set the debug level of the FortiGuard daemon from 0-8.	0
`fortilogd <debug_level_integer>`	Set the debug level of the FortiLog daemon from 0-8.	0
`ipsecd <debug_level_integer>`	Set the debug level of the Internet Key Exchange (IKE) daemon from 0-8.	0
`log-aggregate <debug_level_integer>`	Set the debug level of the log aggregation daemon from 0-8.	0
`log-indexer <debug_level_integer>`	Set the debug level of the log indexer daemon from 0-8.	0
`logfiled <debug_level_integer>`	Set the debug level of the log file daemon from 0-8.	0
`miglogd <debug_level_integer>`	Set the debug level of the miglog daemon from 0-8.	0
`network-summary <debug_level_integer>`	Set the debug level of the network summary daemon from 0-8.	0
`ntpd <debug_level_integer>`	Set the debug level of the Network Time Protocol (NTP) daemon from 0-8.	0
`oftpd <debug_level_integer>`	Set the debug level of the OFTP daemon from 0-8.	0

Variable	Description	Default
`remote-auth <debug_level_integer>`	Set the debug level of the remote authentication daemon from 0-8.	0
`report <debug_level_integer>`	Set the debug level of the report daemon from 0-8.	0
`samba-nfs <debug_level_integer>`	Set the debug level of the Samba and NFS daemon from 0-8.	0
`snmpd <debug_level_integer>`	Set the debug level of the SNMP daemon from 0-8.	0
`sql-integration <debug_level_integer>`	Set the debug level of SQL integration from 0-8.	0
`sqlplugind <debug_level_integer>`	Set the debug level of SQL plugin daemon from 0-8.	0
`sumreportsd <debug_level_integer>`	Set the debug level of sumreport daemon from 0-8.	0
`uploadd <debug_level_integer>`	Set the debug level of upload daemon from 0-8.	0
`vm <debug_level_integer>`	Set the debug level of vulnerability management daemon from 0-8.	0

Example

This example shows how to set the debug level to 5 for the vulnerability management daemon:

```
diagnose debug application vm 5
```

History

4.0 MR2	New.

debug capture-output

Use this command to set capture output type.

Syntax

```
diagnose debug capture-output {clear | disable | enable | show | upload
   <ftp_host_ip>}
```

Variable	Description
`clear`	Clear the capture output file.
`disable`	Disable the capture output.
`enable`	Enable the capture output.
`show`	Display the capture output file content.
`upload <ftp_host_ip>`	Save the capture output file to an FTP server.

Example

This example shows how to upload the capture output file to an FTP server:

```
diagnose debug capture-output upload 192.168.10.1
```

History

4.0 MR2	New.

debug cli

Use this command to set the debug level of CLI.

Syntax

```
diagnose debug cli <integer>
```

Variable	Description	Default
`<integer>`	Set the debug level of CLI from 0-8.	3

Example

This example shows how to set the CLI debug level to 5:

```
diagnose debug cli 5
```

History

4.0 MR2	New.

debug crashlog

Use this command to manage crash logs.

Syntax

```
diagnose debug crashlog clear
diagnose debug crashlog get <aggregation_clt | aggregation_svr | alertd |
   alertmail | archd | auto-rm-files | bin-check | cmdbsvr | cmf | faws |
   fdpd | flgdns | fnbamd | fortilogd | httpsd | hwmond | ipsecd | klogd |
   log-indexer | logfiled | miglogd | newcli | ntpd | oftpd | run-sch-rpt |
   smit | sniffd | snmpd | sumreportsd | uploadd | vmagent | vmpdated>
diagnose debug crashlog list
diagnose debug crashlog upload <aggregation_clt | aggregation_svr | alertd |
   alertmail | archd | auto-rm-files | bin-check | cmdbsvr | cmf | faws |
   fdpd | flgdns | fnbamd | fortilogd | httpsd | hwmond | ipsecd | klogd |
   log-indexer | logfiled | miglogd | newcli | ntpd | oftpd | run-sch-rpt |
   smit | sniffd | snmpd | sumreportsd | uploadd | vmagent | vmpdated>
```

Variable	Description
clear	Delete backtrace and core files.
get <aggregation_clt | aggregation_svr | alertd | alertmail | archd | auto-rm-files | bin-check | cmdbsvr | cmf | faws | fdpd | flgdns | fnbamd | fortilogd | httpsd | hwmond | ipsecd | klogd | log-indexer | logfiled | miglogd | newcli | ntpd | oftpd | run-sch-rpt | smit | sniffd | snmpd | sumreportsd | uploadd | vmagent | vmpdated>	Display the backtrace for an application.
list	List applications that have backtraces or core files.
upload <aggregation_clt | aggregation_svr | alertd | alertmail | archd | auto-rm-files | bin-check | cmdbsvr | cmf | faws | fdpd | flgdns | fnbamd | fortilogd | httpsd | hwmond | ipsecd | klogd | log-indexer | logfiled | miglogd | newcli | ntpd | oftpd | run-sch-rpt | smit | sniffd | snmpd | sumreportsd | uploadd | vmagent | vmpdated>	Save the backtraces and core files of an application to an FTP server.

Example

This example shows how to list applications that have backtraces or core files:

```
diagnose debug crasslog list
```

Output:

```
httpsd:
  btrace.txt: 6404 bytes, Fri Jan  8 09:37:35 EST 2010
  core: 16826368 bytes, Fri Jan  8 09:37:36 EST 2010
```

History

4.0 MR2	New.

debug discardedlog

Use this command to manage discarded logs.

Syntax

```
diagnose debug discardedlog {clear | show | status}
```

Variable	Description
clear	Clear the discarded logs.
show	Display the discarded logs.
status	List the total number of discarded logs and total size of the logs.

Example

This example shows how to list the total number of discarded logs and total size of the logs:

```
diagnose debug discardedlog status
```

Output:

```
Total Num: 8670 Total Size: 7989405
```

History

4.0 MR2	New.

debug info

Use this command to show active debug level settings.

Syntax

```
diagnose debug info
```

History

4.0 MR2	New.

debug output

Use this command to set output type.

Syntax

```
diagnose debug output {disable | enable}
```

Variable	Description
`disable`	Disable the debug output.
`enable`	Enable the debug output.

Example

This example shows how to enable the debug output:

```
diagnose debug output enable
```

History

4.0 MR2	New.

debug report

Use this command to display FortiAnalyzer configuration.

Syntax

```
diagnose debug report
```

History

4.0 MR2	New.

debug reset

Use this command to set all application debug levels to factory default.

Syntax

```
diagnose debug reset
```

History

4.0 MR2	New.

debug timestamp

Use this command to enable or disable debug timestamp.

Syntax

```
diagnose debug timestamp {enable | disable}
```

History

4.0 MR2	New.

device

Use this command to list the type and number of devices monitored by the FortiAnalyzer unit and whether additional devices can be added for each type.

Syntax

```
diagnose device status
```

History

4.0 MR2	New.

dlp-archives

Use this command to manage the quarantined and DLP archived files statistics and show the running status of DLP files.

Syntax

```
diagnose dlp-archives {statistics [flush | show] | status}
```

Variable	Description
`statistics [flush	show]`	Clear or display the quarantined and DLP archived files statistics
`status`	Show the running status of DLP files, including the starting time of the statistics, the file types, the number of files and duplicated files, and the size of the files.

Example

This example shows how to flush the quarantined and DLP archived files statistics:

```
diagnose dlp-archives statistics flush
```

History

4.0 MR2	New.

email

Use this command to detect the email files that cause problems in the archive page and upload them to a server for troubleshooting.

Syntax

```
diagnose email parse <device_name> <service> <ip> <user_name> <password>
   <directory>
```

Variable	Description
`<device_name>`	Enter the name of the device for which you want to parse the email attachments. Enter `all` to parse the email attachments for all devices.
`<service>`	Enter the transfer protocol to be used for sending any problematic emails. The options are ftp, sftp, and scp.
`<ip>`	Enter the IP address of the server for uploading any problematic emails.
`<user_name>`	Enter the user name used for logging in to the server for uploading any problematic emails.
`<password>`	Enter the password used for logging in to the server for uploading any problematic emails.
`<directory>`	Enter the directory on the server for uploading any problematic emails, or press Enter to upload the emails to the default home directory.

Example

This example shows how to parse the emails on a FortiGate unit and send the problematic emails to a server:

```
diagnose email parse FGT4002803033886 ftp 192.168.10.1 admin admin
```

Output:

```
Parsing email archives for device FGT4002803033886
  1238443048:
    Parsing   13 of   13 ...
Totally 13 email(s) parsed, 1/1 email(s) failed parsing uploaded to ftp
   server 192.168.10.1 under home directory.
```

History

4.0 MR2	New.

fortiguard

Use this command to manage the FortiGuard daemon.

Syntax

```
diagnose fortiguard {error-msg [clear | show | upload <ftp_host_ip>] |
    status | vm-refresh}
```

Variable	Description
`error-msg [clear	show	upload <ftp_host_ip>]`	`clear`: Remove the FortiGuard daemon error messages. `show`: Display recent FortiGuard daemon error messages. `upload`: Save the FortiGuard daemon error messages to an FTP server.
`status`	Display the running status of the FortiGuard daemon.
`vm-refresh`	Refresh the vulnerability management FortiGuard network status. This process may take a few minutes.

Example

This example shows how to display the running status of the FortiGuard daemon:

```
diagnose fortiguard status
```

Output:

```
Update Object: VM Engine
         Version: 1.042
         License: Expired
         Last Update Attempt: Thu Jan 14 10:00:40 2010
         Last Update Status: Success
         Update Type: Default Package
Update Object: VM Plugins
         Version: 1.086
         License: Expired
         Last Update Attempt: Thu Jan 14 10:00:40 2010
         Last Update Status: Success
         Update Type: Default Package
```

History

4.0 MR2	New.

fortilogd

Use this command to manage the FortiLog daemon.

Syntax

```
diagnose fortilogd {error-msg [clear | show | upload <ftp_host_ip>] |
    msgrate | msgrate-device | msgrate-total | msgrate-type | msgstat |
    status}
```

Variable	Description
`error-msg [clear | show | upload <ftp_host_ip>]`	`clear`: Remove the FortiLog daemon error messages. `show`: Display recent FortiLog daemon error messages. `upload`: Save the FortiLog daemon error messages to an FTP server.
`msgrate`	Display the message logging rate in the form of messages/second, messages/30seconds, and messages/60seconds.
`msgrate-device`	Display each device's message logging rate in the form of messages/second. The rate for last hour, last day, and last week is listed.
`msgrate-total`	Display all devices' message logging rate in the form of messages/second. The total rate for last hour, last day, and last week is listed.
`msgrate-type`	Display the message logging rate by log type in the form of messages/second. The rate for last hour, last day, and last week is listed.
`msgstat`	Display the message logging status.
`status`	Display the FortiLog daemon running status.

Example

This example shows how to display the running status of the FortiLog daemon:

```
diagnose fortilogd status
```

Output:

```
fortilogd is starting
config socket OK
cmdb socket OK
cmdb register log.device OK
cmdb register log.unregistered OK
cmdb register log.settings OK
cmdb register log.forwarding OK
log socket OK
```

History

4.0 MR2	New.

gui

Use this command to check the web-based manager status.

Syntax

```
diagnose gui console
```

History

4.0 MR2	New.

log

Use this command to view the usage of FortiAnalyzer hard disk space allocated to a device's log and content messages, including quarantined files.

Syntax

```
diagnose log device <device type> <device name>
```

Variable	Description
`<device type>`	Enter the type of device that you want to view the usage of FortiAnalyzer hard disk space allocated to it. Enter FGT, FMG, FML, FCT, or Syslog.
`<device name>`	Enter the name for the device type you select.

Example

This example shows how to display the running status of the FortiLog daemon:

```
diagnose log device FGT FG5A253E07600124
```

Output:

```
Device Name: FG5A253E07600124
Device ID: FG5A253E07600124
Used Space:(logs/DLP/quar/IPS) 1M( 1/ 0/ 0/ 0)
Allocated Space: 1000M
% Used: 0.10%
```

History

4.0 MR2	New.

log-aggregate

Use this command to manage the log aggregation daemon error messages and check its running status.

Syntax

```
diagnose log-aggregate {error-msg [clear | show | upload <ftp_host_ip>] |
   status}
```

Variable	Description
`error-msg [clear	show	upload <ftp_host_ip>]`	`clear`: Remove the log aggregation daemon error messages. `show`: Display recent log aggregation daemon error messages. `upload`: Save the log aggregation daemon error messages to an FTP server.
`status`	Display the log aggregation daemon running status.

Example

This example shows how to display the running status of the log aggregation daemon:

```
diagnose log-aggregate status
```

History

4.0 MR2	New.

log-indexer

Use this command to manage the log indexer daemon.

Syntax

```
diagnose log-indexer bincheck
diagnose log-indexer error-msg [clear | show | upload <ftp_host_ip>]
diagnose log-indexer rebuild-db <device id> <log type>
diagnose log-indexer reindex-all
diagnose log-indexer rebuild-custom <device id> <log type>
diagnose log-indexer reindex-all <device id> <log type>
diagnose log-indexer repair-db <device id> <log type>
diagnose log-indexer report-db
diagnose log-indexer status
```

Variable	Description
`bincheck`	Check the database binary file status.
`error-msg [clear	show	upload <ftp_host_ip>]`	`clear`: Remove the log indexer daemon error messages. `show`: Display recent log indexer daemon error messages. `upload`: Save the log indexer daemon error messages to an FTP server.
`rebuild-db <device id> <log type>`	Rebuild the FortiAnalyzer database for the selected type of logs of a device.
`reindex-all`	Redo the indexing for the log files of all devices.
`rebuild-custom <device id> <log type>`	Redo the indexes that lack the current custom log field for the selected type of logs of a device.
`reindex-all <device id> <log type>`	Redo the indexing for a log type of a device.
`repair-db <device id> <log type>`	Repair the corrupted FortiAnalyzer database for a log type of a device.
`report-db`	Display the number of good and total log files in the database. If the total number is more than the good number, the balance is the number of problematic log files.
`status`	Display the log indexer daemon running status.

Example

This example shows how to display the running status of the log indexer daemon:

```
diagnose log-indexer status
```

Output:

```
sleeping for 13 seconds
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 1 s
          Log file(/Storage/Logs/.sniffer/xlog.log) has more lines than the 
     index.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
Starting to process log files
Compute Work Done: 1 seconds
sleeping for 14 seconds
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
          Index is up to date.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Log file(/Storage/Logs/.sniffer/xlog.log) has more lines than the 
     index.
          Mem: 28340 K, total 2076324 K (1.36%)
          operation took: 0 s
          Binary file is up to date.
```

```
Index is up to date.
Mem: 28340 K, total 2076324 K (1.36%)
operation took: 0 s
Binary file is up to date.
```

History

4.0 MR2 New.

log-xml

Use this command to display log XML build number, version, and checksum.

Syntax

```
diagnose log-xml info
```

Example

This example shows how to display log XML build number, version, and checksum:

```
diagnose log-xml info
```

Output:

```
Log XML build: 0242, Log XML version: 040000, Log XML checksum:
   f5af771633e08febe632d1d06cd4b741
```

History

4.0 MR2 New.

log-checker

Use this command to display the invalid log files for a device.

Syntax

```
diagnose logchecker file <Max invalid logs> <device name> log type {all
   |[racdseghixtvpw]log}
```

Variable	Description
`<Max invalid logs>`	Enter the maximum number of invalid log files to display.

Variable	Description
`<device name>`	Enter the name of the device for which you want to display the invalid log files.
`log type {all |[racdseghixtvpw]log}`	Enter the log type for which you want to display the invalid log files. `r`: application control log `a`: attack log `c`: content log `d`: DLP log `s`: email log `e`: event log `g`: syslog `h`: history log `i`: IM log `x`: network analyzer log `t`: traffic log `v`: virus log `p`: VoIP log `w`: web log

Example

This example shows how to display 5 invalid rlog files for device FG5A253E07600124:

```
diagnose logchecker file 5 FG5A253E07600124 rlog
```

History

4.0 MR2 New.

migration

Use this command to view the migration daemon running status.

Syntax

```
diagnose migration status
```

Example

This example shows how to display the migration daemon running status:

```
diagnose migration status
```

Output 1:

```
Migration has not started.
```

Output 2:

```
Migration is running. (transferring-files) files 7621/7632, size MB 507/616,
    elapsed 00:04:30, remaining 00:00:58
```

Output 3:

```
Migration is finished.
files 7632/7632, size MB 616/616, elapsed 00:07:05, remaining 00:00:00
```

History

4.0 MR2 New.

netlink

Use this command to display the netlink information.

Syntax

```
diagnose netlink device list
diagnose netlink interface list
diagnose netlink ip list
diagnose netlink route list
diagnose netlink rtcache list
diagnose netlink tcp list
diagnose netlink udp list
```

Variable	Description
device list	Display the FortiAnalyzer unit's interface statistics.
interface list	Display the FortiAnalyzer unit's interface status and parameters.
ip list	Display all of the physical and virtual IP addresses associated with the network interfaces of the FortiAnalyzer unit.
route list	Display the FortiAnalyzer unit's routing table contents.
rtcache list	Display the FortiAnalyzer unit's routing cache information.
tcp list	Display the FortiAnalyzer unit's TCP socket information.
udp list	Display the FortiAnalyzer unit's UDP sockets information.

Example

This example shows how to display FortiAnalyzer unit's interface status and parameters.

```
diagnose netlink interface list
```

Output:

```
if=ipsec0 family=00 type=1 index=1 mtu=16260 link=0 master=0
flags=up run noarp
if=ipsec1 family=00 type=65535 index=2 mtu=0 link=0 master=0
flags=noarp
if=ipsec2 family=00 type=65535 index=3 mtu=0 link=0 master=0
flags=noarp
if=ipsec3 family=00 type=65535 index=4 mtu=0 link=0 master=0
flags=noarp
if=port4 family=00 type=1 index=5 mtu=1500 link=0 master=0
flags=broadcast multicast
if=port3 family=00 type=1 index=6 mtu=1500 link=0 master=0
flags=up broadcast multicast
if=port1 family=00 type=1 index=7 mtu=1500 link=0 master=0
flags=up broadcast run multicast
if=port2 family=00 type=1 index=8 mtu=1500 link=0 master=0
flags=up broadcast multicast
if=lo family=00 type=772 index=9 mtu=16436 link=0 master=0
flags=up loopback run
if=tunl0 family=00 type=768 index=10 mtu=1480 link=0 master=0
flags=noarp
if=gre0 family=00 type=778 index=11 mtu=1476 link=0 master=0
flags=noarp
```

History

4.0 MR2	New.

ntpd

Use this command to manage the error messages of the Network Time Protocol daemon (NTPD).

Syntax

```
diagnose ntpd error-msg {clear | show | upload <ftp_host_ip>}
```

Variable	Description
`error-msg {clear	show	upload <ftp_host_ip>}`	`clear`: Remove the NTPD daemon error messages. `show`: Display recent NTPD daemon error messages. `upload`: Save the NTPD daemon error messages to an FTP server.

Example

This example shows how to list the NTPD error messages:

```
diagnose ntpd error-message show
```

Output:

```
[2010-01-14 10:00:27] ERROR: ntpd(397):ntpdate.c:1266: can't find host
   pool.ntp.org
[2010-01-14 08:38:27] ERROR: ntpd(395):ntpdate.c:1266: can't find host
   pool.ntp.org
[2010-01-14 07:38:07] ERROR: ntpd(395):ntpdate.c:1266: can't find host
   pool.ntp.org
[2010-01-14 07:14:34] ERROR: ntpd(396):ntpdate.c:1266: can't find host
   pool.ntp.org
[2010-01-14 06:14:14] ERROR: ntpd(396):ntpdate.c:1266: can't find host
   pool.ntp.org
```

History

4.0 MR2	New.

raid

Use this command to remove disks from the RAID array and show the RAID information.

Syntax

```
diagnose raid delete <disk>}
diagnose raid info
```

Variable	Description
`delete <disk>}`	Enter the number of the disk in the RAID array that you want to delete. The disk number is 1-based.
`info`	Display the RAID information.

Example

This example shows how to list the RAID information on a FortiAnalyzer 800B:

```
diagnose raid info
```

Output:

```
Free Disk Space: 1832.32GB
Total Disk Space: 1833.81GB

RAID information:
RAID level: RAID0
RAID state: OK
RAID controller: Linux MD RAID
Number of disks: 4
Array capacity: 1863.05GB

Disk    State           Size
disk01  OK              465.76GB
disk02  OK              465.76GB
disk03  OK              465.76GB
disk04  OK              465.76GB

MD status:
Personalities : [linear] [raid0] [raid1] [raid10] [raid6] [raid5] [raid4]
   [fault
y]
md0 : active raid0 sda1[0] sdd1[3] sdc1[2] sdb1[1]
      status: OK    member_size: 0
      1953546240 blocks super 1.0 64k chunks

unused devices: <none>
```

History

4.0 MR2	New.

remote-auth

Use this command to manage the remote authentication daemon error messages, test the remote authentication login, and the remote authentication status.

Syntax

```
diagnose remote-auth error-msg {clear | show | upload <ftp_host_ip>}
diagnose remote-auth logintest <user name> <password>
diagnose remote-auth status
```

Variable	Description
`error-msg {clear	show	upload <ftp_host_ip>}`	`clear`: Remove the remote authentication daemon error messages. `show`: Display recent remote authentication daemon error messages. `upload`: Save the remote authentication daemon error messages to an FTP server.

Variable	Description
`logintest <user name> <password>`	Test the login information used by an administrator account for remote authentication.
`status`	Display the running status of the remote authentication daemon.

Example

This example shows the running status of the remote authentication daemon:

```
diagnose remote-auth status
```

Output:

```
Auth group name:auth-group1
Last login status: N/A
```

History

4.0 MR2	New.

report

Use this command to manage the report daemon error messages and show the daemon's running status.

Syntax

```
diagnose report error-msg {clear | show | upload <ftp_host_ip>}
diagnose report status
```

Variable	Description
`error-msg {clear	show	upload <ftp_host_ip>}`	`clear`: Remove the report daemon error messages. `show`: Display recent report daemon error messages. `upload`: Save the report daemon error messages to an FTP server.
`status`	Display the running status of the report daemon.

Example

This example shows the running status of the report daemon:

```
diagnose report status
```

Output:

```
0 reports have been generated successfully, details:
        started          total: 0        scheduled: 0    manually: 0
        finished         successed: 0    killed: 0       failed: 0
        process          running: 0      wait: 0
```

History

4.0 MR2	New.

samba-nfs

Use this command to show the samba-nfs daemon running status.

Syntax

```
diagnose samba-nfs status
```

Example

This example shows the running status of the samba-nfs daemon:

```
diagnose samba-nfs status
```

Output:

```
Samba and NFS running status:
Samba service is running
NFS service is running

Samba version 3.0.5
PID     Username      Group         Machine
--------------------------------------------------------

Service      pid     machine       Connected at
-------------------------------------------------------
No locked files

Server nfs rpc stats:
calls   badcalls        badauth badclnt xdrcall
0       0       0       0       0

Server nfs v2:
null    getattr setattr root    lookup  readlink
0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)
read    wrcache write   create  remove  rename
0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)
link    symlink mkdir   rmdir   readdir fsstat
0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)

Server nfs v3:
null    getattr setattr lookup  access  readlink
0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)
read    write   create  mkdir   symlink mknod
0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)
remove  rmdir   rename  link    readdir readdirplus
0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)  0 (0%)
fsstat  fsinfo  pathconf        commit
0 (0%)  0 (0%)  0 (0%)  0 (0%)
```

History

4.0 MR2	New.

sniffer

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

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

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

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

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

Syntax

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

Variable	Description
<interface_name>	Type the name of a network interface whose packets you want to capture, such as port1, or type any to capture packets on all network interfaces.
'<filter_str>'	Type either none to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as 'tcp port 25'. Surround the filter string in quotes. The filter uses the following syntax: '[[src|dst] host {<host1_fqdn> | <host1_ipv4>}] [and|or] [[src|dst] host {<host2_fqdn> | <host2_ipv4>}] [and|or] [[arp|ip|gre|esp|udp|tcp] port <port1_int>] [and|or] [[arp|ip|gre|esp|udp|tcp] port <port2_int>]' To display only the traffic between two hosts, specify the IP addresses of both hosts. To display only forward or only reply packets, indicate which host is the source, and which is the destination. For example, to display UDP port 1812 traffic between 1.example.com and either 2.example.com or 3.example.com, you would enter: 'udp and port 1812 and src host 1.example.com and dst \(2.example.com or 2.example.com \)'
{1 | 2 | 3}	Type one of the following integers indicating the depth of packet headers and payloads to capture: • 1 for header only • 2 for IP header and payload • 3 for Ethernet header and payload For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (3).
[<count_int>]	Type the number of packets to capture before stopping. If you do not specify a number, the command will continue to capture packets until you press Ctrl + C.

Example

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

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

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

Example

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

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

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

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

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

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

Example

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

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

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

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

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

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

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

To view sniffer output using HyperTerminal and Wireshark

1. Type the sniffer CLI command, such as:

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

2. After you type the sniffer command but ***before*** you press Enter, go to *Transfer* > *Capture Text...*.
3. Select the name and location of the output file, such as `C:\Documents and Settings\username\Fortinet_sniff.txt`.
4. Press Enter to send the CLI command to the FortiAnalyzer unit, beginning packet capture.
5. When you have captured all packets that you want to analyze, press Ctrl + C to stop the capture.
6. Go to *Transfer* > *Capture Text* > *Stop* to stop and save the file.
7. Convert this plain text file to a format recognizable by your network protocol analyzer application.

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

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

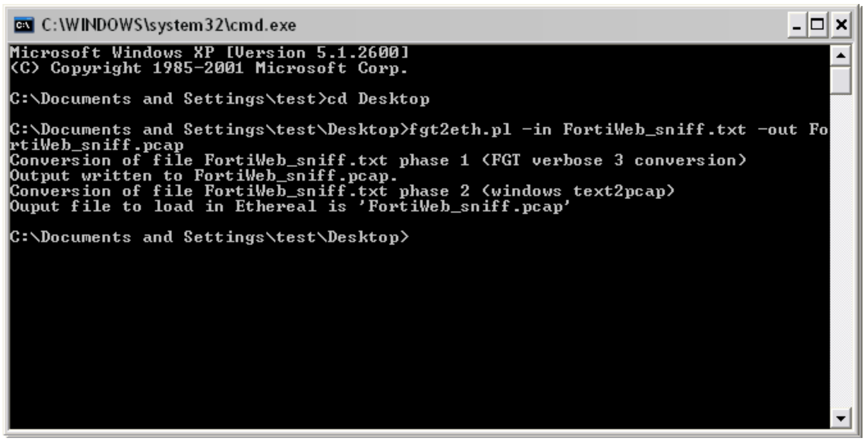
   To use fgt2eth.pl on Windows XP, go to *Start* > *Run* and enter `cmd` to open a command prompt, then enter a command such as the following:

   ```
   fgt2eth.pl -in Fortinet_sniff.txt -out fortianalyzer_sniff.pcap
   ```

   where:

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

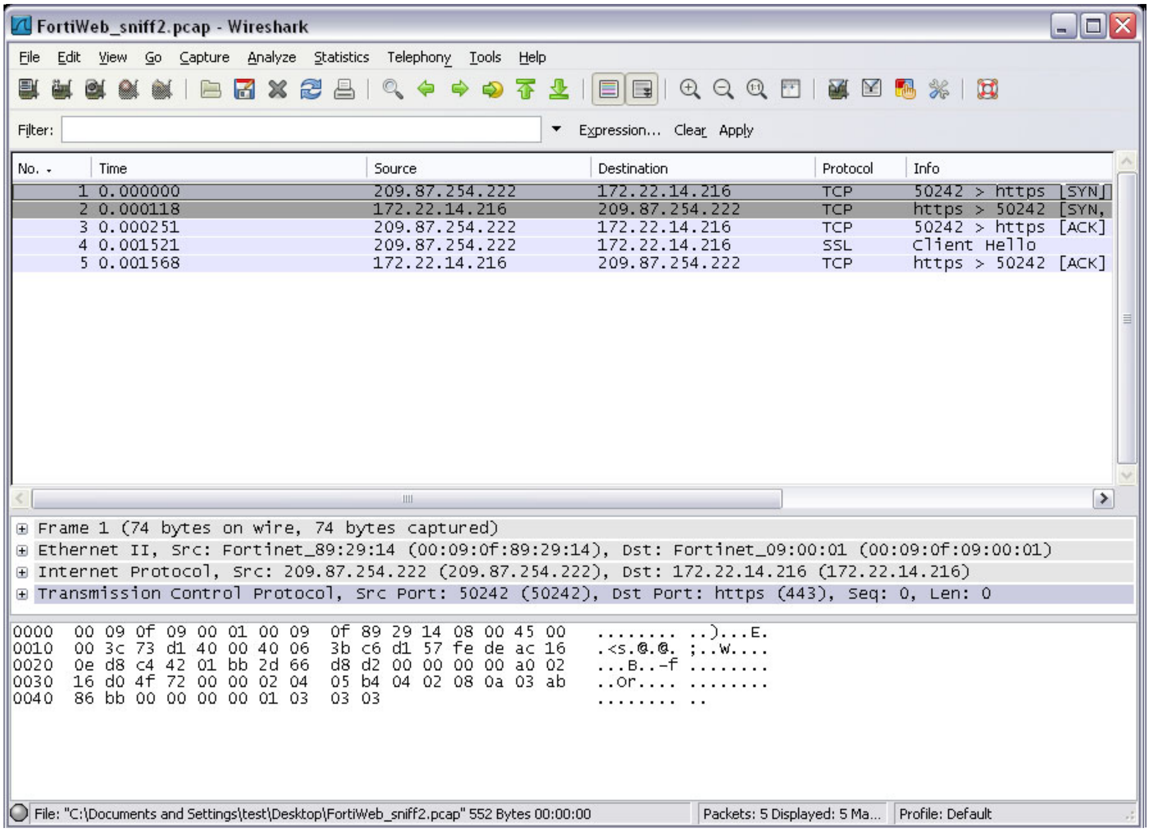
Figure 2: Converting sniffer output to .pcap format



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\test>cd Desktop

C:\Documents and Settings\test\Desktop>fgt2eth.pl -in FortiWeb_sniff.txt -out Fo
rtiWeb_sniff.pcap
Conversion of file FortiWeb_sniff.txt phase 1 (FGT verbose 3 conversion)
Output written to FortiWeb_sniff.pcap.
Conversion of file FortiWeb_sniff.txt phase 2 (windows text2pcap)
Ouput file to load in Ethereal is 'FortiWeb_sniff.pcap'

C:\Documents and Settings\test\Desktop>
```

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

Figure 3: Viewing sniffer output in Wireshark


FortiWeb_sniff2.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	209.87.254.222	172.22.14.216	TCP	50242 > https [SYN]
2	0.000118	172.22.14.216	209.87.254.222	TCP	https > 50242 [SYN,
3	0.000251	209.87.254.222	172.22.14.216	TCP	50242 > https [ACK]
4	0.001521	209.87.254.222	172.22.14.216	SSL	Client Hello
5	0.001568	172.22.14.216	209.87.254.222	TCP	https > 50242 [ACK]

```
⊞ Frame 1 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Fortinet_89:29:14 (00:09:0f:89:29:14), Dst: Fortinet_09:00:01 (00:09:0f:09:00:01)
⊞ Internet Protocol, Src: 209.87.254.222 (209.87.254.222), Dst: 172.22.14.216 (172.22.14.216)
⊞ Transmission Control Protocol, Src Port: 50242 (50242), Dst Port: https (443), Seq: 0, Len: 0
```

```
0000   00 09 0f 09 00 01 00 09  0f 89 29 14 08 00 45 00   ........ ..)...E.
0010   00 3c 73 d1 40 00 40 06  3b c6 d1 57 fe de ac 16   .<s.@.@. ;..W....
0020   0e d8 c4 42 01 bb 2d 66  d8 d2 00 00 00 00 a0 02   ...B..-f ........
0030   16 d0 4f 72 00 00 02 04  05 b4 04 02 08 0a 03 ab   ..Or.... ........
0040   86 bb 00 00 00 00 01 03  03 03                     ........ ..
```

File: "C:\Documents and Settings\test\Desktop\FortiWeb_sniff2.pcap" 552 Bytes 00:00:00 | Packets: 5 Displayed: 5 Ma... | Profile: Default

For additional information on packet capture, see the Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer.

History

4.0 MR2	New.

sys

Use this command to view and manage the system information.

Syntax

```
diagnose sys arp
diagnose sys bios-cert <show>
diagnose sys cpu-mem
diagnose sys dashboard <rebuild-reports>
diagnose sys deviceinfo {ide [drivers | hda | ide0] | nic [ipsec <n> | port
    <n> | lo | tun10 | gre0 | all]}
diagnose sys df
diagnose sys disk {attributes | disable | enable | errors | health |
    identity <disk> | info}
diagnose sys diskusage
diagnose sys file-system {fscheck | fsfix | fsrebuild | fsreport | reset-
    mount-count}
```

```
diagnose sys fsystem
diagnose sys interface <port>
diagnose sys kill <signal> <pid>
diagnose sys pciconfig
diagnose sys sysinfo {cpu | diskused | interrupts | iomem | ioports | memory
   | slab}
diagnose sys top <value>
```

Variable	Description
`arp`	Display the Address Resolution Protocol (ARP) table.
`bios-cert <show>`	Display the availability of BIOS certificate.
`cpu-mem`	Display the usage of CPU and memory.
`dashboard <rebuild-reports>`	Remove and rebuild the widget reports on the dashboard.
`deviceinfo {ide [drivers | hda | ide0] | nic [ipsec <n> | port <n> | lo | tun10 | gre0 | all]}`	Display IDE and NIC information.
`df`	Display file system disk usage information.
`disk {attributes | disable | enable | errors | health | identity <disk> | info}`	`attributes`: Display vendor-specific SMART attributes. `disable`: Disable log disk SMART support. `enable`: Enable log disk SMART support. `errors`: Display SMART error logs. `health`: Display log disk health status. `identity <disk>`: Identify a log disk by blinking its LED. `info`: Display detailed log disk information, including model, serial number, firmware version, and if SMART is enabled.
`diskusage`	Display the disk usage and quota of the FortiAnalyzer unit and each of the registered devices.
`file-system {fscheck | fsfix | fsrebuild | fsreport | reset-mount-count}`	`fscheck`: Check the log disk consistency by rebooting the system. You can view the results using `diagnose file-system fsreport` after the reboot. `fsfix`: Fix non-critical errors on the log disk upon system reboot, and optimize directory structures for ext3 log disk file systems. You can view the results using `diagnose file-system fsreport` after the reboot. `fsrebuild`: Rebuild file system from scratches upon system reboot. This action may cause potential data loss. Do not perform this action unless the `fsfix` report has errors. You can view the results using `diagnose file-system fsreport` after the reboot. `fsreport`: Display the results of the `fscheck`, `fsfix`, and `fsrebuild` commands. `reset-mount-count`: Set the mount-count of log disk to 1 upon system reboot.
`fsystem`	Display the log disk file system information.
`interface <port>`	Display the detailed information for an interface.
`kill <signal> <pid>`	Send a signal to terminate a process that is currently running on the system. • `<signal>` : the signal number to send. • `<pid>`: the process ID where the signal is sent to.
`pciconfig`	Display PCI information.

Variable	Description
`sysinfo {cpu | diskused | interrupts | iomem | ioports | memory | slab}`	`cpu`: Display detailed information for all installed CPU(s). `diskused`: Display the used space and total space of the hard disk. `interrupts`: Display system interrupts information. `iomem`: Display the memory map of I/O ports. `ioports`: Display the address list of I/O ports. `memory`: Display system memory information. `slab`: Display memory allocation information.
`top <value>`	Display the top processes. • `<value>`: the refreshing interval in seconds. The default is 5.

Example

This example shows how to display the interface information of port1:

```
diagnose sys interface port1
```

Output:

```
Interface name                  port1
Link encap                      Ethernet
HWaddr                          00:1D:92:A1:82:AA
inet addr                       172.20.120.138
Bcast                           172.20.120.255
Mask                            255.255.255.0
Status                          up
MTU                             1500
Metric                          1
RX packets                      5689161
errors                          0
droppet                         0
overruns                        0
frame                           0
TX packets                      3226084
errors                          0
droppet                         0
overruns                        0
carrier                         0
collisions                      0
txqueuelen                      100
RX bytes                        536058399 (511.2M Bytes)
TX bytes                        450706417 (429.8M Bytes)
Base address                    0xd000
Memory                          ddd00000-ddd20000
Supported ports                 [ TP ]
Supported link modes            10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
Supports auto-negotiation       Yes
Advertised link modes           10baseT/Half 10baseT/Full
                                100baseT/Half 100baseT/Full
                                1000baseT/Full
Advertised auto-negotiation     Yes
Speed                           100Mb/s
Duplex                          Full
Port                            Twisted Pair
```

```
Physic Address              0
Transceiver                 internal
Auto-negotiation            on
```

History

4.0 MR2	New.

test

Use this command to test the connectivity of the remote LDAP authentication server.

The FortiAnalyzer unit allows you to define a query to retrieve a list of LDAP users from a remote LDAP server. LDAP queries are used in FortiAnalyzer reports as an additional filter for the user field, providing a convenient way for filtering log data without having to list the user names manually.

Syntax

```
diagnose test authentication ldap <server> <user> <password>
```

Variable	Description
`<server> <user> <password>`	Test the remote LDAP authentication server. • `<server>`: the name of the LDAP server. • `<user>`: the LDAP user name used to authenticate an LDAP user. • `<password>`: the LDAP user's password.

Example

This example shows the test result of the LDAP authentication server connectivity:

```
diagnose test authentication ldap ldap1
    cn=administrator,cn=users,dc=dev,dc=qa 123456
```

Output:

```
authenticate 'cn=administrator,cn=users,dc=dev,dc=qa' against 'ldap1'
    succeeded!
```

History

4.0 MR2	New.

upload

Use this command to clear uploading requests and show the upload daemon running status.

Syntax

```
diagnose upload clear {all | failed}
diagnose upload status
```

Variable	Description
`clear {all | failed}`	Clear all or failed uploading requests.
`status`	Display the running status of the upload daemon.

Example

This example shows the running status of the upload daemon:

```
diagnose upload status
```

Output:

```
Uploading queue...
        Request 0,  retries:3
                File0 : FWF50B3G07526100-elog.1263492172.log-2010-01-15-12-
   58-26
        Request 1,  retries:3
                File0 : FL800B3908000420-elog.1263578416.log-2010-01-15-13-
   00-16
        Request 2,  retries:3
                File0 : FMG3KB3F09000109-elog.1263492114.log-2010-01-15-12-
   58-33
        Request 3,  retries:3
                File0 : FWF50B3G07526100-tlog.1263492396.log-2010-01-15-12-
   58-12
        Request 4,  retries:3
                File0 : FG5A253E06500088-elog.1263492050.log-2010-01-15-12-
   55-53
        Request 5,  retries:3
                File0 : FG5A253E07600124-elog.1263492050.log-2010-01-15-12-
   55-52
        Request 6,  retries:3
                File0 : FGT50B3G06500085-tlog.1263492199.log-2010-01-15-12-
   56-33
End of uploading queue.
```

History

4.0 MR2	New.

vm

Use this command to manage the vulnerability management (VM) daemon.

Syntax

```
diagnose vm downgrade {disable | enable}
diagnose vm engine-log
diagnose vm error-msg {clear | show | upload <ftp_host_ip>}
diagnose vm status
```

Variable	Description
`downgrade {disable | enable}`	Enable or disable downgrading the VM engine.
`engine-log`	Display VM engine logs.
`error-msg {clear | show | upload <ftp_host_ip>}`	`clear`: Remove the VM daemon error messages. `show`: Display recent VM daemon error messages. `upload`: Save the VM daemon error messages to an FTP server.
`status`	Display the running status of the VM daemon.

Example

This example shows the running status of the VM daemon:

```
diagnose vm status
```

Output:

```
Currently no running schedule.
Scan schedule(s) queued:
        None.
Map schedule(s) queued:
        None.
Compliance jobs:
        None.
```

History

4.0 MR2	New.

vpn

Use this command to list the information about the FortiAnalyzer IPSec gateway and the VPN tunnel between a device and the FortiAnalyzer unit.

Syntax

```
diagnose vpn gw list <intf_name> <port No.>
diagnose tunnel list
```

Variable	Description
`list <intf_name> <port No.>`	Display the interface name and port number of the FortiAnalyzer IPSec gateway used for the VPN tunnel between a device and the FortiAnalyzer unit.
`list`	Display the information of the VPN tunnel between a device and the FortiAnalyzer unit.

History

4.0 MR2	New.

show

The show commands display a part of your FortiAnalyzer unit's configuration in the form of commands that are required to achieve that configuration from the firmware's default state.

Note: Although not explicitly shown in this section, for all config commands, there are related get and show commands which display that part of the configuration. get and show commands use the same syntax as their related config command, unless otherwise mentioned. For syntax examples and descriptions of each configuration object, field, and option, see 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:

```
FortiAnalyzer# show system dns
config system dns
  set primary 172.16.1.10
  set secondary 0.0.0.0
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 been reverted to its default value.

Appendix: FortiAnalyzer Web Services

The FortiAnalyzer unit provides Web Services to allow FortiManager units to remotely manage the FortiAnalyzer unit. Web Services also facilitate retrieving information from the FortiAnalyzer unit or running scripts on the FortiAnalyzer unit by third party tools. The FortiAnalyzer Web Service APIs are XML-based, using WC3 Web Services Description Language (WSDL).

This section describes how to use Web Services with third party tools. For information on using Web Services with the FortiManager unit, see the *FortiAnalyzer Administration Guide*.

This section includes:

- Connecting to FortiAnalyzer Web Services
- Getting information from the FortiAnalyzer unit
- Interacting with the FortiAnalyzer unit
- Example: Searching and retrieving FortiGate IPS packet logs

Connecting to FortiAnalyzer Web Services

To start working with Web Services on your FortiAnalyzer unit, you need to enable Web Services and obtain the Web Services Description Language (WSDL) file that defines the XML requests you can make and the responses that FortiAnalyzer can provide. You must also configure login credentials for the third party tools.

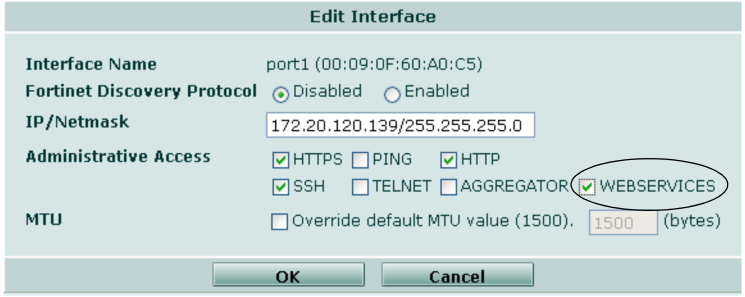
Enabling Web Services

You must enable Web Services on the network interfaces to which Web Services clients will connect.

To enable Web Services on an interface - web-based manager

1. Go to *System* > *Network* > *Interface*.
2. Select the *Edit* icon for the interface that you want to use.
3. In the *Administrative Access* section, select *WEBSERVICES*.
4. Select *OK*.

Figure 4: Enabling web services



Interface Name	port1 (00:09:0F:60:A0:C5)
Fortinet Discovery Protocol	● Disabled ○ Enabled
IP/Netmask	172.20.120.139/255.255.255.0
Administrative Access	☑ HTTPS □ PING ☑ HTTP ☑ SSH □ TELNET □ AGGREGATOR ☑ WEBSERVICES
MTU	□ Override default MTU value (1500). 1500 (bytes)

To enable Web Services on an interface - CLI

1 Enter the following CLI commands:

```
config system interface
  edit <port>
    set allowaccess webservice
  end
```

where `<port>` is the network interface that you want to use for Web Services.

The `allowaccess` command should also include the other types of administrative access that you want to permit. For example, to allow HTTPS, SSH, and Web Services, enter the command `set allowaccess https ssh webservice`.

The FortiAnalyzer unit handles Web Services requests on port 8080.

Obtaining the WSDL file

Download the WSDL file directly from the following URL:
https://<FortiAnalyzer_ip_address>:8080/FortiAnalyzerWS?wsdl

The following is a section of the WSDL file:

```
<definitions name="FortiAnalyzerWS"
targetNamespace="http://localhost:8080/FortiAnalyzerWS.wsdl">
  <types>
      <schema targetNamespace="urn:FortiAnalyzerWS"
         elementFormDefault="qualified"
         attributeFormDefault="qualified">
        <import
           namespace="http://schemas.xmlsoap.org/soap/encoding/"/
           >
        <element name="FortiRequestEl" type="ns:FortiRequest"/>
        <element name="FortiResponseEl" type="ns:FortiResponse"/>
        <!-- enumerations -->
        <simpleType name="SearchContent">
          <restriction base="xsd:string">
            <enumeration value="Logs"/>
            <enumeration value="ContentLogs"/>
            <enumeration value="LocalLogs"/>
          </restriction>
        </simpleType>
        <simpleType name="ReportType">
          <restriction base="xsd:string">
            <enumeration value="FortiGate"/>
            <enumeration value="FortiClient"/>
            <enumeration value="FortiMail"/>
          </restriction>
        </simpleType>
        …
  <service name="FortiAnalyzerWS">
    <documentation>gSOAP 2.7.7 generated service
       definition</documentation>
      <port name="FortiAnalyzerWS" binding="tns:FortiAnalyzerWS">
        <SOAP:address location="https://localhost:8080/FortiAnalyzerWS"
           />
      </port>
  </service>
</definitions>
```

Getting information from the FortiAnalyzer unit

Using the following the APIs, you can obtain information from the FortiAnalyzer unit, such as:

- Requesting search logs or DLP archives (FortiAnalyzerSearch)
- Requesting archives (FortiAnalyzerGetArchive)
- Requesting the quarantine repository (FortiAnalyzerQuarantineRepository)
- Getting the FortiAnalyzer configuration (FortiGetConfigurations)
- Listing reports (FortiAnalyzerListGeneratedReports)
- Getting reports (FortiAnalyzerGetGeneratedReport)
- Getting the system status (FortiAnalyzerGetSystemStatus)

Requesting search logs or DLP archives (`FortiAnalyzerSearch`)

Use this API to search the following three types of contents:

- Logs (SearchContent=Logs) -- searches the FortiGate logs
- ContentLogs (SearchContent=ContentLogs) -- searches the archives
- LocalLogs (SearchContent=LocalLogs) -- searches the FortiAnalyzer logs

For the FortiGate log search, you can search the following FortiGate log types:

Table 11: FortiGate log types

Event	Traffic	Attack	Antivirus
WebLogs	IM	Email	Content
History	Generic	VoIP	DLP
AppCtrl			

For the FortiGate content/archive search, you can search the following archive types:

Table 12:

Web	Email	FTP	Quarantine
IM	MMS	IPS	

For more details, see the WSDL file.

The following example request searches the FTP archives of a FortiGate device. Note that the request envelope and header have been removed for clarity.

Example request:

```
<ns2:FortiAnalyzerSearch>
   <ns2:Content>ContentLogs</ns2:Content>
   <ns2:Format>XML</ns2:Format>
   <ns2:Compression>None</ns2:Compression>
   <ns2:DeviceName>FGT2002801000000</ns2:DeviceName>
   <ns2:LogType>Content</ns2:LogType>
   <ns2:SearchCriteria>itime&gt;0
       itime&lt;2158963206</ns2:SearchCriteria>
   <ns2:MaxNumMatches>100</ns2:MaxNumMatches>
   <ns2:StartIndex>1</ns2:StartIndex>
   <ns2:CheckArchive>1</ns2:CheckArchive>
   <ns2:DLPArchiveType>FTP</ns2:DLPArchiveType>
```

```
</ns2:FortiAnalyzerSearch>
```

Example response:

```
<ns2:FortiResponse>
  <ns2:FortiAnalyzerSearchResult>
    <ns2:TotalResultsFound>1</ns2:TotalResultsFound>
    <ns2:MatchesReturned>1</ns2:MatchesReturned>
    <ns2:StartIndex>1</ns2:StartIndex>
    <ns2:Logs>
      <ns2:Data>
        <ns2:cLog>
          <ns2:itime>1251750977</ns2:itime>
          <ns2:device_id>FGT2002801000000</ns2:device_id>
          <ns2:log_id>32776</ns2:log_id>
          <ns2:type>contentlog</ns2:type>
          <ns2:subtype>FTP</ns2:subtype>
          <ns2:pri>information</ns2:pri>
          <ns2:vd>root</ns2:vd>
          <ns2:cstatus>clean</ns2:cstatus>
          <ns2:user>N/A</ns2:user>
          <ns2:group>N/A</ns2:group>
          <ns2:endpoint>N/A</ns2:endpoint>
          <ns2:SN>450963</ns2:SN>
          <ns2:c_filename>1021526847:5</ns2:c_filename>
          <ns2:NonDefFields>
          <ns2:name>device_id</ns2:name>
          <ns2:value>FGT2002801000000</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>log_id</ns2:name>
          <ns2:value>32776</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>subtype</ns2:name>
          <ns2:value>FTP</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>type</ns2:name>
          <ns2:value>contentlog</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>timestamp</ns2:name>
          <ns2:value>1251750929</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>pri</ns2:name>
          <ns2:value>information</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>itime</ns2:name>
          <ns2:value>1251750977</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>vd</ns2:name>
          <ns2:value>root</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>epoch</ns2:name>
          <ns2:value>1021526847</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>eventid</ns2:name>
          <ns2:value>5</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>infection</ns2:name>
          <ns2:value>block</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>client</ns2:name>
          <ns2:value>10.10.1.101</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>server</ns2:name>
          <ns2:value>172.20.110.103</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>rcvd</ns2:name>
          <ns2:value>5</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>sent</ns2:name>
          <ns2:value>0</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>dlp_sensor</ns2:name>
          <ns2:value>log_content</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>ftpcmd</ns2:name>
          <ns2:value>RETR</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>file</ns2:name>
          <ns2:value>asd.exe</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>clogver</ns2:name>
          <ns2:value>3</ns2:value>
        </ns2:NonDefFields>
        <ns2:NonDefFields>
          <ns2:name>virus</ns2:name>
          <ns2:value>N/A</ns2:value>
        </ns2:NonDefFields>
      </ns2:cLog>
    </ns2:Data>
  </ns2:Logs>
```

```
</ns2:FortiAnalyzerSearchResult>
```

Requesting archives (FortiAnalyzerGetArchive)

Use this API to retrieve the archives.

Example request:

```
<ns2:FortiAnalyzerGetArchive>
  <ns2:Type>Quarantine</ns2:Type>
  <ns2:DeviceID>FG36002805000000</ns2:DeviceID>
  <ns2:FileName></ns2:FileName>
  <ns2:Checksum>fa10</ns2:Checksum>
  <ns2:Compression>None</ns2:Compression>
</ns2:FortiAnalyzerGetArchive>
```

Example response:

```
<ns2:FortiAnalyzerArchiveData>
  <ns2:ArchiveFile>VGhpcyBpcyBhbiBpbmZlY3RlZCBmaWxlIQ</ns2:Archiv
     eFile>
</ns2:FortiAnalyzerArchiveData>
```

Requesting the quarantine repository (FortiAnalyzerQuarantineRepository)

Use this API to access the quarantine files.

Example request:

```
<ns2:FortiAnalyzerQuarantineRepository>
  <ns2:DeviceID>FG36002805033343</ns2:DeviceID>
  <ns2:MaxNumMatches>100</ns2:MaxNumMatches>
  <ns2:StartIndex>1</ns2:StartIndex>
  <ns2:Type>0,1,2</ns2:Type>
  <ns2:Service>FTP,IMAP</ns2:Service>
  <ns2:FilterMask>0</ns2:FilterMask>
</ns2:FortiAnalyzerQuarantineRepository>
```

Example response:

```
<ns2:FortiAnalyzerQuarantineRepositoryResult>
  <ns2:TotalResultsFound>38</ns2:TotalResultsFound>
  <ns2:MatchesReturned>37</ns2:MatchesReturned>
  <ns2:StartIndex>1</ns2:StartIndex>
  <ns2:Quarantines>
    <ns2:DeviceName>FG36002805000000</ns2:DeviceName>
    <ns2:FileName>oink64009</ns2:FileName>
    <ns2:StartTime>2009-09-22T21:04:07Z</ns2:StartTime>
    <ns2:EndTime>2009-09-23T18:21:07Z</ns2:EndTime>
    <ns2:Service>IMAP</ns2:Service>
    <ns2:Checksum>fa09</ns2:Checksum>
    <ns2:Reason>Suspicious</ns2:Reason>
    <ns2:Status>Infected</ns2:Status>
    <ns2:DuplicateCount>3</ns2:DuplicateCount>
    <ns2:Size>27</ns2:Size>
  </ns2:Quarantines>
  …
</ns2:FortiAnalyzerQuarantineRepositoryResult>
```

Getting the FortiAnalyzer configuration (`FortiGetConfigurations`)

Use this API to retrieve the FortiAnalyzer configuration file.

Example request:

```
<ns2:FortiGetConfigurations></ns2:FortiGetConfigurations>
```

Example response:

```
<ns2:FortiGetConfigurationsResults>
  <ns2:Configurations>
    #config-version=FLG800-4.00-FW-build0050-
091015:opmode=0:vdom=0:user=admin
    #conf_file_ver=0
    #buildno=0050
    …
  </ns2:Configurations>
</ns2:FortiGetConfigurationsResults>
```

Listing reports (`FortiAnalyzerListGeneratedReports`)

Use this API to get a list of log reports without report contents.

Example request:

```
<ns2:FortiAnalyzerListGeneratedReports>
  <ns2:Type>FortiGate</ns2:Type>
  <ns2:CreateDateStart>1970-01-01T00:00:00Z</ns2:CreateDateStart>
  <ns2:CreateDateEnd>2031-02-16T21:05:50Z</ns2:CreateDateEnd>
</ns2:FortiAnalyzerListGeneratedReports>
```

Example response:

```
<ns2:FortiAnalyzerGeneratedReportsList>
  <ns2:TotalNumberExists>11</ns2:TotalNumberExists>
  <ns2:ReportList>
    <ns2:GeneratedReport>Web_2009-04-12-
       1912</ns2:GeneratedReport>
    <ns2:StartTime>2009-04-12T18:12:14Z</ns2:StartTime>
    <ns2:EndTime>2009-04-12T18:12:16Z</ns2:EndTime>
    <ns2:ReportProgressPercent>100</ns2:ReportProgressPercent>
    <ns2:Size>0</ns2:Size>
    <ns2:Formats>H</ns2:Formats>
  </ns2:ReportList>
  …
</ns2:FortiAnalyzerGeneratedReportsList>
```

Getting reports (`FortiAnalyzerGetGeneratedReport`)

Use this API to get report contents.

Example request:

```
<ns2:FortiAnalyzerGetGeneratedReport>
  <ns2:Type>FortiGate</ns2:Type>
  <ns2:ReportName>Bandwidth_Analysis-2009-10-06-
     2043</ns2:ReportName>
  <ns2:Compression>None</ns2:Compression>
```

```
</ns2:FortiAnalyzerGetGeneratedReport>
```

Example response:

```
<ns2:FortiAnalyzerReportData>
  <ns2:RptContent>Report_content_stripped</ns2:RptContent>
</ns2:FortiAnalyzerReportData>
```

Getting the system status (`FortiAnalyzerGetSystemStatus`)

Use this API to get the FortiAnalyzer system status.

Example request:

```
<ns2:FortiAnalyzerGetSystemStatus></ns2:FortiAnalyzerGetSystemStat
```

Example response:

```
<ns2:FortiAnalyzerSystemStatusResults>
  <ns2:SerialNumber>FLG8002704000000</ns2:SerialNumber>
  <ns2:UpTime>0 day 17 hour 53 min</ns2:UpTime>
  <ns2:HostName>FortiAnalyzer-800</ns2:HostName>
  <ns2:FirmwareVersion>FortiAnalyzer-800 v4.0,build0050
(Interim)</ns2:FirmwareVersion>
  <ns2:LicenseInfo_RVSEngine>1.30 Wed Jul 15 23:51:00
2009&#xA;</ns2:LicenseInfo_RVSEngine>
  <ns2:LicenseInfo_RVPPlugins>1.65 Wed Jul 15 23:51:00
2009&#xA;</ns2:LicenseInfo_RVPPlugins>

<ns2:DeviceLicense_FortiGateSyslogs_reg>13</ns2:DeviceLicense_Fort
iGateSyslogs_reg>

<ns2:DeviceLicense_FortiGateSyslogs_unreg>0</ns2:DeviceLicense_For
tiGateSyslogs_unreg>

<ns2:DeviceLicense_FortiManagers_reg>1</ns2:DeviceLicense_FortiMan
agers_reg>

<ns2:DeviceLicense_FortiManagers_unreg>0</ns2:DeviceLicense_FortiM
anagers_unreg>
  <ns2:SystemResources_mem>29</ns2:SystemResources_mem>
  <ns2:SystemResources_cpu>0</ns2:SystemResources_cpu>
  <ns2:SystemResources_HD>0</ns2:SystemResources_HD>
  <ns2:NumRaidDisks>4</ns2:NumRaidDisks>
  <ns2:RaidLevel>raid 0</ns2:RaidLevel>
  <ns2:RaidDisk>
    <ns2:DiskNum>1</ns2:DiskNum>
    <ns2:MemberOfRaid>Yes</ns2:MemberOfRaid>
    <ns2:Status>OK</ns2:Status>
    <ns2:Size>114473</ns2:Size>
  </ns2:RaidDisk>
  <ns2:RaidDisk>
    <ns2:DiskNum>2</ns2:DiskNum>
    <ns2:MemberOfRaid>Yes</ns2:MemberOfRaid>
    <ns2:Status>OK</ns2:Status>
    <ns2:Size>114498</ns2:Size>
  </ns2:RaidDisk>
  <ns2:RaidDisk>
    <ns2:DiskNum>3</ns2:DiskNum>
    <ns2:MemberOfRaid>Yes</ns2:MemberOfRaid>
    <ns2:Status>OK</ns2:Status>
    <ns2:Size>114498</ns2:Size>
  </ns2:RaidDisk>
  <ns2:RaidDisk>
    <ns2:DiskNum>4</ns2:DiskNum>
    <ns2:MemberOfRaid>Yes</ns2:MemberOfRaid>
    <ns2:Status>OK</ns2:Status>
    <ns2:Size>114498</ns2:Size>
  </ns2:RaidDisk>
  <ns2:DiskSpaceFree>447576</ns2:DiskSpaceFree>
  <ns2:DiskSpaceUsed>3192</ns2:DiskSpaceUsed>
</ns2:FortiAnalyzerSystemStatusResults>
```

Interacting with the FortiAnalyzer unit

You can work on the FortiAnalyzer unit itself by:

- Running a report (FortiAnalyzerRun)
- Uploading a language (FortiAnalyzerUploadLanguageFile)
- Setting the FortiAnalyzer configuration (FortiSetConfigurations)
- Removing archives (FortiAnalyzerRemoveArchive)

Running a report (FortiAnalyzerRun)

Use this API to generate a log report immediately.

Example request:

```
<ns2:FortiAnalyzerRun>
  <ns2:Type>FortiGateReport</ns2:Type>
  <ns2:Name>rpt1</ns2:Name>
</ns2:FortiAnalyzerRun>
```

Example response

```
<ns2:FortiAnalyzerRunResults>
  <ns2:Status>InProgress</ns2:Status>
  <ns2:NewReportName>rpt1-2009-10-16-1524</ns2:NewReportName>
</ns2:FortiAnalyzerRunResults>
```

Uploading a language (FortiAnalyzerUploadLanguageFile)

Use this API to upload a language file to the FortiAnalyzer unit.

Example request:

```
<ns2:FortiAnalyzerUploadLanguageFile>
  <ns2:name>mylang</ns2:name>
  <ns2:formatFile>Format_File_to_upload</ns2:formatFile>
  <ns2:stringFile>String_File_to_upload</ns2:stringFile>
</ns2:FortiAnalyzerUploadLanguageFile>
```

Example response:

```
<ns2:FortiResponseStatus>Success</ns2:FortiResponseStatus>
```

Setting the FortiAnalyzer configuration (`FortiSetConfigurations`)

Use this API to upload a configuration script to the FortiAnalyzer unit.

Example request:

```
<ns2:FortiSetConfigurations>
  <ns2:Configurations>
    config system interface
    edit "port1"
    set ip 192.168.1.99 255.255.255.0
    set allowaccess ping https ssh http aggregator
    next
    edit "port2"
    set ip 172.20.110.101 255.255.255.0
    set allowaccess ping https ssh http aggregator webservice
    next
    end
    </ns2:Configurations>
</ns2:FortiSetConfigurations>
```

Example response:

```
<ns2:FortiSetConfigurationsResults>
  <ns2:Status>Success</ns2:Status>
  <ns2:ErrorLineNumber>0</ns2:ErrorLineNumber>
</ns2:FortiSetConfigurationsResults>
```

Removing archives (`FortiAnalyzerRemoveArchive`)

Use this API to delete DLP archive and quarantine files.

Example request:

```
<ns2:FortiAnalyzerRemoveArchive>
  <ns2:Type>Quarantine</ns2:Type>
  <ns2:DeviceID>FG36002805000000</ns2:DeviceID>
  <ns2:Vdom></ns2:VDom>
  <ns2:FileName></ns2:FileName>
  <ns2:Checksum></ns2:Checksum>
</ns2:FortiAnalyzerRemoveArchive>
```

Example: Searching and retrieving FortiGate IPS packet logs

If you have enabled FortiGate IPS packet logging to the FortiAnalyzer unit, you can use FortiAnalyzer web services to search and retrieve packet logs.

To do this, you must first search through the FortiGate logs to locate the attack logs for a specific FortiGate device, using the `FortiAnalyzerSearch` API.

Example request:

```
<ns2:FortiAnalyzerSearch>
  <ns2:Content>Logs</ns2:Content>
  <ns2:Format>XML</ns2:Format>
  <ns2:Compression>None</ns2:Compression>
  <ns2:DeviceName>FGT2002801000000</ns2:DeviceName>
  <ns2:LogType>Attack</ns2:LogType>
  <ns2:SearchCriteria></ns2:SearchCriteria>
  <ns2:MaxNumMatches>100</ns2:MaxNumMatches>
  <ns2:StartIndex>1</ns2:StartIndex>
  <ns2:CheckArchive>0</ns2:CheckArchive>
  <ns2:DLPArchiveType></ns2:DLPArchiveType>
</ns2:FortiAnalyzerSearch>
```

After you get the search results, you can retrieve the packet log file using the `FortiAnalyzerGetArchive` API.

Note that the file name of the packet log is the value of the `incident_serialno` field returned in the response.

Example request:

```
<ns2:FortiAnalyzerGetArchive>
  <ns2:Type>IPS</ns2:Type>
  <ns2:DeviceID>FGT2002801000000</ns2:DeviceID>
  <ns2:FileName>incident_serialno</ns2:FileName>
  <ns2:Checksum></ns2:Checksum>
  <ns2:Compression>None</ns2:Compression>
</ns2:FortiAnalyzerGetArchive>
```

Example response:

```
<ns2:FortiAnalyzerArchiveData>
  <ns2:ArchiveFile>content_of_packet_log</ns2:ArchiveFile>
</ns2:FortiAnalyzerArchiveData>
```

Index

FORTINET®

www.fortinet.com

FORTINET®

www.fortinet.com