



# FortiScan<sup>®</sup>

Version 4.0.0

CLI Reference Guide



## **FortiScan CLI Reference Guide**

Version 4.0.0

7 July 2010

17-400-126827-20100707

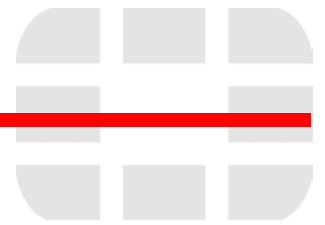
© Copyright 2010 Fortinet, Inc. All rights reserved. No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet, Inc.

### **Trademarks**

Dynamic Threat Prevention System (DTPS), APSecure, FortiAnalyzer, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiScan, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

### **Regulatory compliance**

FCC Class A Part 15 CSA/CUS



# Contents

---

<b>Introduction</b>	<b>7</b>
Registering your Fortinet product . . . . .	7
Customer service and technical support . . . . .	7
Training . . . . .	7
Documentation . . . . .	8
Conventions . . . . .	8
About this document . . . . .	9

---

<b>Using the CLI</b>	<b>11</b>
Connecting to the CLI . . . . .	11
Command syntax . . . . .	14
Sub-commands . . . . .	17
Tips and Tricks . . . . .	19

---

<b>config</b>	<b>21</b>
gui console . . . . .	21
report output . . . . .	22
system console . . . . .	24
system dns . . . . .	25
system fips . . . . .	26
system fortiguard . . . . .	27
system global . . . . .	29
system interface . . . . .	30
system mail . . . . .	32
system ntp . . . . .	33
system raid . . . . .	34
system route . . . . .	35
system snmp . . . . .	36
vm business-risk . . . . .	38
vm map-config . . . . .	42
vm scan-profile . . . . .	45

vm schedule . . . . .	47
vm sensor. . . . .	49

---

**execute** **53**

backup . . . . .	54
disconnect . . . . .	55
em_dbbackup. . . . .	56
em_dbrestore. . . . .	58
factoryreset . . . . .	60
ping . . . . .	61
ping-options. . . . .	62
reboot. . . . .	64
reload . . . . .	65
restore . . . . .	66
set-date . . . . .	68
set-time . . . . .	69
shutdown . . . . .	70
traceroute . . . . .	71
upload-benchmark . . . . .	72
vm . . . . .	73

---

**get** **75**

system performance . . . . .	76
system status . . . . .	77

---

**diagnose** **79**

alertmail. . . . .	79
cmdb . . . . .	80
debug application. . . . .	81
debug capture-output. . . . .	83
debug cli . . . . .	84
debug crashlog . . . . .	85
debug emdb . . . . .	86
debug emserver . . . . .	88
debug info . . . . .	90

debug output . . . . .	91
debug report . . . . .	92
debug reset . . . . .	93
debug timestamp . . . . .	94
fortiguard . . . . .	95
gui . . . . .	96
netlink. . . . .	97
ntpd . . . . .	99
raid . . . . .	100
sniffer . . . . .	103
sys . . . . .	108
vm . . . . .	111
vpn . . . . .	112

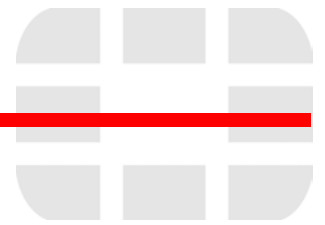
---

<b>show</b>	<b>113</b>
-------------	------------

---

<b>Index</b>	<b>115</b>
--------------	------------





# Introduction

The FortiScan Appliance is a network appliance that identifies security vulnerabilities and finds compliance exposures on hosts, servers and throughout the network transparently. It enables you to perform network discovery, asset prioritization and profile-based scanning.

It also delivers patch management with ready-to-deploy remediation and enforcement actions, allowing network managers to change configurations and potentially mitigate weak settings, including disabling an application or denying a network request.

This document describes how to use the FortiScan Command Line Interface (CLI) to manage and configure the FortiScan Appliance.

This section describes:

- [Registering your Fortinet product](#)
- [Customer service and technical support](#)
- [Training](#)
- [Documentation](#)
- [Conventions](#)

## 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](mailto: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](mailto:techdoc@fortinet.com).

## Conventions

Fortinet technical documentation uses the conventions described in this section.

### 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
<b>Button, menu, text box, field, or check box label</b>	From <i>Minimum log level</i> , select <i>Notification</i> .
<b>CLI input*</b>	<pre>config system dns   set primary &lt;address_ipv4&gt; end</pre>
<b>CLI output</b>	<pre>FSC-3000C # get system settings comments           : (null) opmode             : nat</pre>
<b>Emphasis</b>	HTTP connections are <b>not</b> secure and can be intercepted by a third party.
<b>File content</b>	<pre>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt; &lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</pre>
<b>Hyperlink</b>	Visit the Fortinet Technical Support web site, <a href="https://support.fortinet.com">https://support.fortinet.com</a> .
<b>Keyboard entry</b>	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
<b>Navigation</b>	Go to <code>VPN &gt; IPSEC &gt; Auto Key (IKE)</code> .
<b>Publication</b>	For details, see the <a href="#">FortiScan Administration Guide</a> .

\* For conventions used to represent command syntax, see “[Command syntax](#)” on page 14.

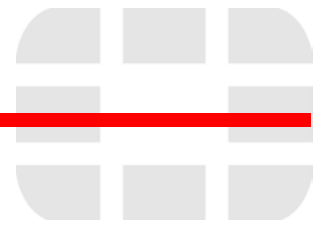
## About this document

This document describes how to use the FortiScan Command Line Interface (CLI). This document contains the following chapters:

- [Using the CLI](#) describes how to connect to and use the FortiScanCLI.
- [config](#) describes commands used to configure basic features.
- [execute](#) describes execute commands used to run maintenance and other tasks, such as backups, pings, or vulnerability scans.
- [get](#) describes commands that display a part of your FortiScan unit’s configuration in the form of a list of settings and their values.
- [diagnose](#) describes commands that display diagnostic information that help you to troubleshoot problems.
- [show](#) describes commands that display a part of your FortiScan unit’s configuration in the form of commands that are required to achieve that configuration from the firmware’s default state.



**Note:** Diagnose commands are used for gathering detailed information useful to Fortinet technical support for debugging. Contact Fortinet technical support before using diagnose commands.



# 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](#)
- [Tips and Tricks](#)



**Note:** Each FortiScan user account is assigned a role at the time of creation, and each role contains a specific set of permissions to perform some or all the FortiScan CLI commands. Your user account may not permit you to perform all of the CLI commands described in this chapter. Generally speaking, administrators have full access to CLI commands, while operator and auditors have very limited access to CLI commands through Web CLI console only. For details, see “Feature RBAC (Roles)” in the [FortiScan Administration Guide](#) or see your FortiScan Administrator for more information.

## 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 FortiScan Appliance unit’s console port. Network access is when you remotely access the CLI using SSH or Telnet client software. Connecting to the console or network connection varies by FortiScan Appliance model. See the [FortiScan QuickStart Guide](#) shipped with your FortiScan Appliance unit to verify which cable to use.

Local access is required if:

- You are installing your FortiScan Appliance 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 [FortiScan QuickStart Guide](#) for your FortiScan Appliance model.
- 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 through which users will be accessing the CLI.

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 FortiScan model).
- terminal emulation software, such as HyperTerminal for Windows.

See the [FortiScan QuickStart Guide](#) for your FortiScan Appliance model to verify which cable is correct.

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 FortiScan unit

- 1 Connect the FortiScan unit's console port to the communications port on your management computer using the null modem or RJ-45 to DB-9 cable (whichever is correct for your FortiScan Appliance model).
- 2 Verify that the FortiScan 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 FortiScan 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*.

<b>Bits per second</b>	9600
<b>Data bits</b>	8
<b>Parity</b>	None
<b>Stop bits</b>	1
<b>Flow control</b>	None

- 10 Press Enter to connect to the FortiScan 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 FortiScan CLI from the Internet or any other unprotected network.

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

You must enable Secure 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 FortiScan Appliance unit with a static route to a router that can forward packets from the FortiScan Appliance 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 the FortiScan Appliance” chapter in the *FortiScan 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.
- 5 Type `end` and press Enter to save the changes to the FortiScan configuration.
- 6 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 FortiScan unit to accept SSH connections, you can use an SSH client on your management computer to connect to the FortiScan CLI.

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

### To connect to the CLI using SSH

- 1 Start an SSH client.
- 2 Connect to a FortiScan 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 FortiScan model name followed by a # is displayed:

```
FortiScan-1000B #
```

You can now enter CLI commands.



**Note:** FortiScan 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 FortiScan CLI from the Internet or any other unprotected network.

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

### To connect to the CLI using Telnet

- 1 Start a Telnet client.
- 2 Connect to a FortiScan 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 FortiScan model name followed by a # is displayed:

```
FortiScan-1000B #
```

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.

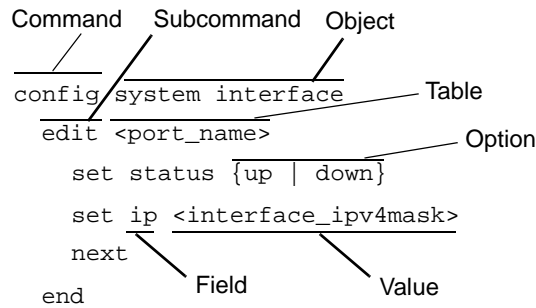
### Terminology

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



- **command** – A word that begins the command line and indicates an action that the FortiScan Appliance 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 FortiScan Appliance 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
<b>Square brackets</b> [ ]	<p>A non-required word or series of words. For example:</p> <pre>[verbose {1   2   3}]</pre> <p>indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as:</p> <pre>verbose 3</pre>
<b>Angle brackets</b> < >	<p>A word constrained by data type.</p> <p>To define acceptable input, the angled brackets contain a descriptive name followed by an underscore ( <code>_</code> ) and suffix that indicates the valid data type. For example:</p> <pre>&lt;retries_int&gt;</pre> <p>indicates that you should enter a number of retries, such as 5.</p> <p>Data types include:</p> <ul style="list-style-type: none"> <li>• <code>&lt;xxx_name&gt;</code>: A name referring to another part of the configuration, such as <code>policy_A</code>.</li> <li>• <code>&lt;xxx_index&gt;</code>: An index number referring to another part of the configuration, such as 0 for the first static route.</li> <li>• <code>&lt;xxx_pattern&gt;</code>: A regular expression or word with wild cards that matches possible variations, such as <code>*@example.com</code> to match all email addresses ending in <code>@example.com</code>.</li> <li>• <code>&lt;xxx_fqdn&gt;</code>: A fully qualified domain name (FQDN), such as <code>mail.example.com</code>.</li> <li>• <code>&lt;xxx_email&gt;</code>: An email address, such as <code>admin@mail.example.com</code>.</li> <li>• <code>&lt;xxx_url&gt;</code>: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <code>http://www.fortinet./com/</code>.</li> <li>• <code>&lt;xxx_ipv4&gt;</code>: An IPv4 address, such as <code>192.168.1.99</code>.</li> <li>• <code>&lt;xxx_v4mask&gt;</code>: A dotted decimal IPv4 netmask, such as <code>255.255.255.0</code>.</li> <li>• <code>&lt;xxx_ipv4mask&gt;</code>: A dotted decimal IPv4 address and netmask separated by a space, such as <code>192.168.1.99 255.255.255.0</code>.</li> <li>• <code>&lt;xxx_ipv4/mask&gt;</code>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as <code>192.168.1.99/24</code>.</li> <li>• <code>&lt;xxx_ipv4range&gt;</code>: A hyphen ( <code>-</code> )-delimited inclusive range of IPv4 addresses, such as <code>192.168.1.1-192.168.1.255</code>.</li> <li>• <code>&lt;xxx_str&gt;</code>: A string of characters that is <b>not</b> another data type, such as <code>P@ssw0rd</code>. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences. See <a href="#">"Special characters" on page 19</a>.</li> <li>• <code>&lt;xxx_int&gt;</code>: An integer number that is <b>not</b> another data type, such as 15 for the number of minutes.</li> </ul>

Table 2: Command syntax notation (Continued)

<b>Curly braces { }</b>	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 [ ].
<b>Options delimited by vertical bars  </b>	Mutually exclusive options. For example: {enable   disable} indicates that you must enter either <code>enable</code> or <code>disable</code> , but must not enter both.
<b>Options delimited by spaces</b>	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: <code>ping https ssh</code> <b>Note:</b> To change the options, you must re-type the entire list. For example, to add <code>snmp</code> to the previous example, you would type: <code>ping https snmp ssh</code> 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 interface
```

the command prompt becomes:

```
[interface] #:
```

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 15](#).

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

<b>delete</b> <b>&lt;table&gt;</b>	Remove a table from the current object. delete is only available within objects containing tables.
<b>edit &lt;table&gt;</b>	Create or edit a table in the current object. 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.
<b>end</b>	Save the changes to the current object and exit the config command. This returns you to the top-level command prompt.
<b>get</b>	List the configuration of the current object or table. <ul style="list-style-type: none"> <li>In objects, get lists the table names (if present), or fields and their values.</li> <li>In a table, get lists the fields and their values.</li> </ul>
<b>purge</b>	Remove all tables in the current object. purge is only available for objects containing tables. <b>Caution:</b> Back up the FortiScan Appliance unit before performing a purge. purge cannot be undone. To restore purged tables, the configuration must be restored from a backup. For details, see <a href="#">"execute backup" on page 54</a> . <b>Caution:</b> 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 FortiScan Appliance unit to be formatted and restored.
<b>rename</b> <b>&lt;table&gt; to</b> <b>&lt;table&gt;</b>	Rename a table. rename is only available within objects containing tables.
<b>show</b>	Display changes to the default configuration. Changes are listed in the form of configuration commands.

Table 4: Commands for fields

<b>abort</b>	Exit both the edit and/or config commands without saving the fields.
<b>end</b>	Save the changes made to the current table or object fields, and exit the config command. (To exit without saving, use abort instead.)
<b>get</b>	List the configuration of the current object or table. <ul style="list-style-type: none"> <li>In objects, get lists the table names (if present), or fields and their values.</li> <li>In a table, get lists the fields and their values.</li> </ul>
<b>next</b>	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.
<b>set &lt;field&gt;</b> <b>&lt;value&gt;</b>	Set a field's value. <b>Note:</b> 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.
<b>show</b>	Display changes to the default configuration. Changes are listed in the form of configuration commands.
<b>unset</b> <b>&lt;field&gt;</b>	Reset the table or object's fields to default values.

## 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 5: 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 (backslash).

**Table 6: 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.

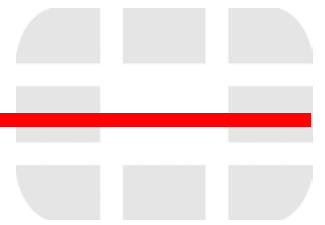
For example, the host name must not contain special characters, and so the CLI will not accept most symbols and other encoded characters as input when configuring the host name. This means that languages other than English often cannot be used; however, dictionary profiles support terms encoded in UTF-8,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

It is best to use only ASCII characters when configuring the FortiScan Appliance 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 FortiScan Appliance unit using non-ASCII characters, verify that all systems interacting with the FortiScan Appliance 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 browser or Telnet/SSH client while you work.



# config

Use the `config` commands to modify the FortiScan Appliance configurations. This chapter describes the following `config` commands:

<code>gui console</code>	<code>system global</code>	<code>system snmp</code>
<code>report output</code>	<code>system interface</code>	<code>vm business-risk</code>
<code>system console</code>	<code>system mail</code>	<code>vm map-config</code>
<code>system dns</code>	<code>system ntp</code>	<code>vm scan-profile</code>
<code>system fips</code>	<code>system raid</code>	<code>vm schedule</code>
<code>system fortiguard</code>	<code>system route</code>	<code>vm sensor</code>

## 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
<code>preferences &lt;filedata&gt;</code>	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

4.0.0	New.
-------	------

## report output

Use this command to configure an output template to be used in a network scan 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}
    set upload-compress {disable | enable}
  end
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

Keywords and variables	Description	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
upload-pass <password>	Enter the password for accessing the server.	No default
upload-dir <dir_path>	Enter the directory path where the FortiScan Appliance 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 FortiScan Appliance unit's hard disk once it has been completely uploaded to the remote server.	disable
upload-compress {disable   enable}	Enable or disable gzip compression when uploading the completed report.	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_fscan
    set upload-compress enable
  end
end

```

## History

**4.0.0**                      New.

## 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 <code>show</code> or <code>get</code> commands only.	standard

### Example

In this example, the baud rate is set to 9600.

```
config system console
  set baudrate 9600
end
```

### History

**4.0.0**                      New.

## system dns

Use this command to set a primary and alternate DNS server address. For features which use domain names, the FortiScan 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 FortiScan DNS server IP address is set to 172.16.35.133 and the secondary FortiScan 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
```

### History

**4.0.0**                      New.

## system fips

Use this command to set the FortiScan 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 FortiScan firmware. To obtain this 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 FortiScan 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 FortiScan unit.	disable

### Example

In this example, the FortiScan Appliance FIPS-CC mode operation is set to `enable`.

```
config system fips
  set status enable
end
```

### History

**4.0.0**                      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
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

Keywords and variables	Description	Default
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

**4.0.0**                      New.

## system global

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

### Syntax

```
config system global
  set admintimeout <timeout_int>
  set hostname <host_str>
  set language {english}
  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. <b>Note:</b> Sessions will not time out when viewing real-time logs.	5
hostname <host_str>	Type a name for this FortiScan unit.	FortiScan model name.
language {english}	Set the web-based manager display language.	english
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_scanner
end
```

### History

**4.0.0**                      New

## system interface

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

### Syntax

```
config system interface
  edit <interface_str>
    set allowaccess <access_str>
    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
end
```

Keywords and variables	Description	Default
<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 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.
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
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 FortiScan 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 192.168.100.159 255.255.255.0
end
end
```

### History

**4.0.0**                  New

## system mail

Use this command to add or modify an SMTP email server user account to enable the FortiScan unit to send alert messages using email.



**Note:** This command applies only for network scan vulnerability alert messages. For compliance management alert messages, you should configure an email server from the web-based manager's *System > Server Settings > Email Notification* page.

### Syntax

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

### History

**4.0.0**                      New.

## system ntp

Use this command to configure Network Time Protocol (NTP) servers.

### Syntax

```
config system ntp
  set ntpsync {enable | disable}
  set syncinterval <interval_int>
  config ntpserver
    edit <serverid_int>
      set server <IPv4_addr>[/<hostname_str>]
    end
  end
end
```

Keywords and variables	Description	Default
ntpsync {enable   disable}	Enable synchronization of the FortiScan unit's system time with the ntp server.	disable
syncinterval <interval_int>	Enter the interval in minutes between contacting NTP server to synchronize time. The range is from 1 to 1440 minutes. This setting is only valid when ntpsync is enabled.	0
config ntpserver	Configure multiple NTP servers.	
<serverid_int>	Enter the number for this NTP server.	
server <IPv4_addr>[/<hostname_str>]	Enter the IPv4 address and hostname (optional) for this NTP server.	

### Example

This example shows how to add an NTP server with IP address 172.17.93.49.

```
config system ntp
  set ntpsync enable
  set syncinterval 100
  config ntpserver
    edit server1
      set ip 172.17.93.49
    end
  end
end
```

### History

**4.0.0** New.

## system raid

Use the this command to configure RAID levels.

### Syntax

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

Keywords and variables	Description	Default
level [raid10   raid0   raid1   raid5]	Enter the level of RAID you want for your FortiScan unit. <b>Note:</b> Raid level depends on the number of hard drives available.	No default

### Example

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

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

### History

**4.0.0**                      New.

## system route

Use these commands to configure static routes.

### Syntax

```
config system route
  edit <sequence_int>
    set device {port1 | port2 | port3 | port4 }
    set dst <destination_ip-mask>
    set gateway <gateway_ip>
  end
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 FortiScan forwarding table.	No default.
device {port1   port2   port3   port4 }	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
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 | system_event |
      raid }
    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   system_event   raid }	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
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

<b>4.0.0</b>	New
--------------	-----

## 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 *Network Scan > 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 FortiScan 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

Variables	Description	Default
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
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

4.0.0 New.

## Related commands

- [vm schedule](#)

## 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-port-adtn <string>
    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 <code>grp-update</code> is enabled. You must specify an asset group with the <code>asset-group</code> command before configuring this setting.	disable
hour <hour_int>	Specify when during the day a scheduled scan will run. Use this command with <code>minute</code> to specify an exact time.	12
ip-range <ipv4>	Enter the IP address range the FortiScan unit scans.	No default
live-host-sweep {enable   disable}	Enable to have the FortiScan unit discover live hosts in the IP address range specified with the <code>ip-range</code> 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 <code>hour</code> 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. <ul style="list-style-type: none"> <li><code>daily</code> has the FortiScan unit run the scan once a day. Use the <code>hour</code> and <code>minute</code> commands to specify when during the day the scan is run.</li> <li><code>weekly</code> has the FortiScan unit run the scan once a week. Use the <code>day-of-week</code>, <code>hour</code>, and <code>minute</code> commands to specify when during the week the scan is run.</li> <li><code>monthly</code> has the FortiScan unit run the scan once a month. Use the <code>day-of-month</code>, <code>hour</code>, and <code>minute</code> commands to specify when during the month the scan is run.</li> </ul>	daily
schedule {run-now   run-later}	Specify whether the schedule will run once or at regular intervals. <ul style="list-style-type: none"> <li><code>run-now</code> will have the FortiScan unit run the specified map configuration immediately, and only once.</li> <li><code>run-later</code> will have the FortiScan unit run the map configuration at regular intervals, as specified with the <code>recurrence</code> command.</li> </ul>	run-now
tcp-port-adtn <string>	Enter any ports you want scanned in addition to those specified with the <code>tcp-standard-scan</code> command. Enter individual ports separating by commas. Enter port ranges, separating the start and end ports with a dash. For example, set <code>tcp-port-adtn 10,12,14,20-30</code>	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

Variables	Description	Default
udp-port-adtn <string>	Enter any ports you want scanned in addition to those specified with the <code>udp-standard-scan</code> command. Enter individual ports separating by commas. Enter port ranges, separating the start and end ports with a dash. For example, set <code>udp-port-adtn 100,115,200-250,9500</code>	No default
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

**4.0.0**            New.

## 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 FortiScan unit to 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 FortiScan 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 <code>tcp-port-grp</code> command. Enter individual ports separating by commas. Enter port ranges, separating the start and end ports with a dash. For example, set <code>tcp-port-adtn 10,12,14,20-30</code>	No default
tcp-port-grp {full   standard   light   none}	Select the type of TCP port scan the VM scan will execute. <ul style="list-style-type: none"> <li>• <code>full</code> scans all TCP ports. This is the most thorough scan, but it also takes the longest.</li> <li>• <code>standard</code> scans about 1800 of the most commonly used TCP ports.</li> <li>• <code>light</code> scans about 160 of the most commonly used TCP ports.</li> <li>• <code>none</code> disables the TCP port scan.</li> </ul>	none

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

**4.0.0**                      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

Variables	Description	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. <ul style="list-style-type: none"> <li>daily has the FortiScan unit run the scan once a day. Use the hour and minute commands to specify when during the day the scan is run.</li> <li>weekly has the FortiScan unit 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.</li> <li>monthly has the FortiScan unit 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.</li> </ul>	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. <ul style="list-style-type: none"> <li>run-now will have the FortiScan unit run the schedule immediately, and only once.</li> <li>run-later will have the FortiScan unit run the schedule at regular intervals, as specified with the recurrence command.</li> </ul>	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

4.0.0 New.

## Related commands

- [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
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 FortiScan 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

Variables	Description	Default
bug {existent   ignore   nonexistent}	Include vulnerabilities depending on whether they've been assigned a Bug Traq ID. <ul style="list-style-type: none"> <li>• <code>existent</code> - restrict the included vulnerabilities to only those with a Bug Traq ID.</li> <li>• <code>nonexistent</code> - restrict the included vulnerabilities to only those without a Bug Traq ID.</li> <li>• <code>ignore</code> - do not restrict the included vulnerabilities based on whether they have been assigned a Bug Traq ID.</li> </ul>	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 <code>all</code> 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. <ul style="list-style-type: none"> <li>• <code>existent</code> - restrict the included vulnerabilities to only those with a CVE ID.</li> <li>• <code>nonexistent</code> - restrict the included vulnerabilities to only those without a CVE ID.</li> <li>• <code>ignore</code> - do not restrict the included vulnerabilities based on whether they have been assigned a CVE ID.</li> </ul>	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. <ul style="list-style-type: none"> <li>• <code>yes</code> - restrict the included vulnerabilities to only those that have been detected in previous scans using this sensor.</li> <li>• <code>no</code> - restrict the included vulnerabilities to only those that have not been detected in previous scans using this sensor.</li> <li>• <code>ignore</code> - do not restrict the vulnerabilities included in the filter based on whether they have been detected in previous scans using this sensor.</li> </ul>	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. <ul style="list-style-type: none"> <li>existent - restrict the included vulnerabilities to only those that are FortiGuard IPS signatures.</li> <li>nonexistent - restrict the included vulnerabilities to only those that are not FortiGuard IPS signatures.</li> <li>ignore - do not restrict the included vulnerabilities based on whether they are FortiGuard IPS signatures.</li> </ul>	ignore
patch {existent   ignore   nonexistent}	Include vulnerabilities depending on whether a patch exists to fix them. <ul style="list-style-type: none"> <li>existent - restrict the included vulnerabilities to only those with a patch.</li> <li>nonexistent - restrict the included vulnerabilities to only those without a patch.</li> <li>ignore - do not restrict the included vulnerabilities based on whether they have a patch.</li> </ul>	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 <i>Vendor Reference</i> column of the vulnerability database. <ul style="list-style-type: none"> <li>existent - restrict the included vulnerabilities to only those with a link.</li> <li>nonexistent - restrict the included vulnerabilities to only those without a link.</li> <li>ignore - do not restrict the included vulnerabilities based on whether they have a vendor reference link.</li> </ul>	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
  end
```

end

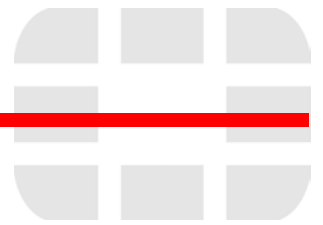
## History

4.0.0

New.

## Related commands

- [vm scan-profile](#)



# execute

The `execute` commands perform immediate operations on the FortiScan 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`
- update vulnerability management services.

This chapter contains the following sections:

<a href="#">backup</a>	<a href="#">reload</a>
<a href="#">disconnect</a>	<a href="#">restore</a>
<a href="#">em_dbbackup</a>	<a href="#">set-date</a>
<a href="#">em_dbrestore</a>	<a href="#">set-time</a>
<a href="#">factoryreset</a>	<a href="#">shutdown</a>
<a href="#">ping</a>	<a href="#">traceroute</a>
<a href="#">ping-options</a>	<a href="#">upload-benchmark</a>
<a href="#">reboot</a>	<a href="#">vm</a>

# backup

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

## Syntax

```
execute backup config {[ftp | sftp | scp | tftp] <address_ipv4>
<arg_1> <arg_2> <arg_3> <arg_4>}
execute backup config-secure {[ftp | sftp | scp | tftp]
<address_ipv4> <arg_1> <arg_2> <arg_3> <arg_4>}
```

Keywords and variables	Description
config {[ftp   sftp   scp   tftp] <address_ipv4> <arg_1> <arg_2> <arg_3> <arg_4>}	Back up the system configuration to a file on an FTP, SFTP, SCP, or TFTP server, where: <ul style="list-style-type: none"> <li>• &lt;address_ipv4&gt; – The IP address of the server.</li> <li>• &lt;arg_1&gt; – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename.</li> <li>• &lt;arg_2&gt; – For FTP, SFTP or SCP enter a password or enter '-'. For TFTP enter the filename or press Enter.</li> <li>• &lt;arg_3&gt; – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter.</li> <li>• &lt;arg_4&gt; – Enter a filename or press Enter.</li> </ul> <b>Note:</b> 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] <address_ipv4> <arg_1> <arg_2> <arg_3> <arg_4>}	Back up an encrypted system configuration file to a FTP, SFTP, SCP, or TFTP server, where: <ul style="list-style-type: none"> <li>• &lt;address_ipv4&gt; – The IP address of the server.</li> <li>• &lt;arg_1&gt; – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename.</li> <li>• &lt;arg_2&gt; – For FTP, SFTP or SCP enter a password or enter '-'. For TFTP enter the filename or press Enter.</li> <li>• &lt;arg_3&gt; – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter.</li> <li>• &lt;arg_4&gt; – Enter a filename or press Enter.</li> </ul> <b>Note:</b> 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 FortiScan-3000C system configuration to a file named fsc3000c.cfg to a TFTP server at IP address 192.168.1.23.

```
execute backup config tftp fsc3000c.cfg 192.168.1.23 *****
```

## History

4.0.0 New

## disconnect

Use this command to disconnect an administrator from the FortiScan 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 who is logged in to the web-based manager is:

```
execute disconnect 1
```

### History

<b>4.0.0</b>	New
--------------	-----

## em\_dbbackup

Use this command to back up the FortiScan Appliance database.



**Note:** Backing up the FortiScan appliance database and the Appliance configuration settings require different commands. To perform a full system backup, first backup the Appliance configuration settings using the `execute backup` command. Then backup the database using the `execute em_dbbackup` command.



**Note:** Backing up the database shuts down the application server. The system reboots automatically after the backup completes.

### Syntax

```
execute em_dbbackup {[ftp | sftp | scp | tftp] <address_ipv4>
  <arg_1> <arg_2> <arg_3> <arg_4>}
```

Keywords and variables	Description
<pre>em_dbbackup {[ftp   sftp   scp   tftp] &lt;address_ipv4&gt; &lt;arg_1&gt; &lt;arg_2&gt; &lt;arg_3&gt; &lt;arg_4&gt;}</pre>	<p>Back up the system database to a file on a FTP, SFTP, SCP, or TFTP server, where:</p> <ul style="list-style-type: none"> <li>• <code>&lt;address_ipv4&gt;</code> - The IP address of the server where the backup file is to be stored.</li> <li>• <code>&lt;arg_1&gt;</code> - For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename.</li> <li>• <code>&lt;arg_2&gt;</code> - For FTP, SFTP or SCP enter a password or enter <code>'.'</code>. For TFTP enter the filename or press Enter.</li> <li>• <code>&lt;arg_3&gt;</code> - For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter.</li> <li>• <code>&lt;arg_4&gt;</code> - Enter a filename or press Enter.</li> </ul> <p><b>Note:</b> Use the FTP server's IP address whenever you are entering the FTP server information. Using a domain name is not supported.</p>

### Example

The following backs up a FortiScan 3000C database to a file FSC3000CDB to a FTP server at IP address 172.17.94.96:

```
exec em_dbbackup ftp 172.17.94.96 henrydu - ./ FSC3000CDB
```

A confirmation message appears:

```
This operation will stop web service and backup database to the
specified file!
Do you want to continue? (y/n)y
```

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

```
Shutting down application server...
Dumping database...
Compressing...
```

```
build_no
dbbackup.dat
Connect to ftp server 172.17.94.96 ...
```

```
Successfully uploaded the backup file to ftp server
172.17.94.96.
Reboot system immediately.
```

A confirmation message appears:

```
This operation will reboot the system.
Do you want to continue? (y/n)y
```

If you select to continue by entering *y*, the system will reboot.



**Note:** If you don't want to continue by entering *n*, the system application server will not start up and you will be unable to use the FortiScan web-based manager.

## History

4.0.0	New.
-------	------

## em\_dbrestore

Use this command to restore the FortiScan Appliance database.



**Note:** Restoring the FortiScan appliance database and the Appliance configuration settings require different commands. To perform a full system restore, first restore the Appliance configuration settings using the `execute restore` command. Then restore the database using the `execute em_dbrestore` command.



**Note:** Restoring the database shuts down the application server. The system reboots automatically after the restore operation completes.

### Syntax

```
execute em_dbrestore {[ftp | sftp | scp | tftp] <address_ipv4>
  <arg_1> <arg_2> <arg_3> <arg_4>}
```

Keywords and variables	Description
<pre>em_dbrestore {[ftp   sftp   scp   tftp] &lt;address_ipv4&gt; &lt;arg_1&gt; &lt;arg_2&gt; &lt;arg_3&gt; &lt;arg_4&gt;}</pre>	<p>Restore the system database from a file on a FTP, SFTP, SCP, or TFTP server, where:</p> <ul style="list-style-type: none"> <li>• <code>&lt;address_ipv4&gt;</code> - The IP address of the server where the backup file is located.</li> <li>• <code>&lt;arg_1&gt;</code> - For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename.</li> <li>• <code>&lt;arg_2&gt;</code> - For FTP, SFTP or SCP enter a password or enter <code>'.'</code>. For TFTP enter the filename or press Enter.</li> <li>• <code>&lt;arg_3&gt;</code> - For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter.</li> <li>• <code>&lt;arg_4&gt;</code> - Enter a filename or press Enter.</li> </ul> <p><b>Note:</b> Use the FTP server's IP address whenever you are entering the FTP server information. Using a domain name is not supported.</p>

### Example

The following command restores a FortiScan 3000C database from a file FSC3000CDB located on the FTP server at IP address 172.17.94.96:

```
exec em_dbrestore ftp 172.17.94.96 henrydu - ./ FSC3000CDB
```

A confirmation message appears:

```
This operation will stop the web service and restore the
  database to the specified file!
Do you want to continue? (y/n)y
```

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

```
Connect to ftp server 172.17.94.96 ...
Successfully downloaded the file from ftp server 172.17.94.96.
Shutting down application server...
```

```
Uncompressing...
build_no
```

```
dbbackup.dat
Restoring database...

You are now connected to database "postgres".

SET
SET
...
Successfully restore the database.

Reboot system immediately.
A confirmation message appears:
This operation will reboot the system.
Do you want to continue? (y/n)y
If you select to continue by entering y, the system will reboot.
```



**Note:** If you don't want to continue by entering n, the system application server will not start up and you will be unable to use the FortiScan web-based manager.

## History

4.0.0	New.
-------	------

## factoryreset



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

Use this command to reset the FortiScan configuration to the firmware's default settings.

### Syntax

```
execute factoryreset
```

### History

4.0.0	New
-------	-----

## ping

Use this command to send an ICMP echo request (ping) to test the network connection between the FortiScan 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
```

### History

<b>4.0.0</b>	New
--------------	-----

## ping-options

Use this command to set ICMP echo request (ping) options to control the way ping tests the network connection between the FortiScan 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.
repeat-count <repeats_int>	Specify how many times to repeat ping.	5
source {auto   <source-intf_ip>}	Specify the FortiScan interface from which to send the ping. If you specify auto, the FortiScan 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 FortiScan 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. <ul style="list-style-type: none"> <li>lowdelay = minimize delay</li> <li>throughput = maximize throughput</li> <li>reliability = maximize reliability</li> <li>lowcost = minimize cost</li> <li>default = 0</li> </ul>	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 FortiScan interface with IP address 192.168.10.23.

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

## History

<b>4.0.0</b>	New
--------------	-----

## reboot

Use this command to restart the FortiScan unit.

### Syntax

```
execute reboot
```

### History

<b>4.0.0</b>	New
--------------	-----

## reload

Use this command to reload the FortiScan unit configuration.

### Syntax

```
execute reload
```

### History

<b>4.0.0</b>	New
--------------	-----

## restore

Use this command to:

- restore configuration backups
- change the FortiScan firmware
- restore the VM package from a specified server.

### Syntax

```
execute restore image {[ftp | sftp | scp | tftp] <address_ipv4>
  <arg_1> <arg_2> <arg_3> <arg_4>}
execute restore config {[ftp | sftp | scp | tftp] <address_ipv4>
  <arg_1> <arg_2> <arg_3> <arg_4>}
execute restore config-secure {[ftp | sftp | scp | tftp]
  <address_ipv4> <arg_1> <arg_2> <arg_3> <arg_4>}
execute restore vm {[ftp | sftp | scp | tftp] <address_ipv4>
  <arg_1> <arg_2> <arg_3> <arg_4>}
```

Variables	Description
image {[ftp   sftp   scp   tftp] <address_ipv4> <arg_1> <arg_2> <arg_3> <arg_4>}	<p>Upload a firmware image from an FTP, SFTP, SCP or TFTP server to the FortiScan unit, where:</p> <ul style="list-style-type: none"> <li>• &lt;address_ipv4&gt; - The IP address of the server where the firmware image is located.</li> <li>• arg_1 - For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename.</li> <li>• arg_2 - For FTP, SFTP or SCP enter a password or enter '.'. For TFTP enter the filename or press Enter.</li> <li>• arg_3 - For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter.</li> <li>• arg_4 - Enter a filename or press Enter.</li> </ul> <p>The FortiScan unit reboots, loading the new firmware.</p>
config {[ftp   sftp   scp   tftp] <address_ipv4> <arg_1> <arg_2> <arg_3> <arg_4>}	<p>Restore the system configuration from a backup file on an FTP, SFTP, SCP or TFTP server, where:</p> <ul style="list-style-type: none"> <li>• &lt;address_ipv4&gt; - The IP address of the server where the backup file is located.</li> <li>• arg_1 - For FTP, SFTP or SCP enter a user name. For TFTP enter a directory.</li> <li>• arg_2 - For FTP, SFTP or SCP enter a password or enter '.'. For TFTP enter the filename.</li> <li>• arg_3 - For FTP, SFTP or SCP enter a directory. For TFTP, press Enter.</li> <li>• arg_4 - Enter a filename and press Enter.</li> </ul> <p>The new configuration replaces the existing configuration, including administrator accounts and passwords.</p>

Variables	Description
<pre>config-secure {[ftp   sftp   scp   tftp] &lt;address_ipv4&gt; &lt;arg_1&gt; &lt;arg_2&gt; &lt;arg_3&gt; &lt;arg_4&gt;}</pre>	<p>Restore the system configuration from an encrypted backup configuration file on an FTP, SFTP, SCP or TFTP server, where:</p> <ul style="list-style-type: none"> <li>• &lt;address_ipv4&gt; - The IP address of the server where the backup file is located.</li> <li>• arg_1 - For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename.</li> <li>• arg_2 - For FTP, SFTP or SCP enter a password or enter '-'. For TFTP enter the filename or press Enter.</li> <li>• arg_3 - For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter.</li> <li>• arg_4 - Enter a filename or press Enter.</li> </ul> <p>The new configuration replaces the existing configuration, including administrator accounts and passwords.</p>
<pre>vm {[ftp   sftp   scp   tftp] &lt;address_ipv4&gt; &lt;arg_1&gt; &lt;arg_2&gt; &lt;arg_3&gt; &lt;arg_4&gt;}</pre>	<p>Restore vulnerabilities from an FTP, SFTP, SCP or TFTP server, where:</p> <ul style="list-style-type: none"> <li>• &lt;address_ipv4&gt; - The IP address of the server where the vulnerabilities file is located.</li> <li>• arg_1 - For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename.</li> <li>• arg_2 - For FTP, SFTP or SCP enter a password or enter '-'. For TFTP enter the filename or press Enter.</li> <li>• arg_3 - For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter.</li> <li>• arg_4 - Enter a filename or press Enter.</li> </ul>

## Example

The following example uploads a configuration file from a TFTP server to the FortiScan unit and restarts the FortiScan 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
```

## History

**4.0.0**                      New.

## set-date

Use this command to set the system date.

### Syntax

```
execute set-date <date_str>
```

The variable `<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 2010:

```
execute set-date 17/03/2010
```

### History

<b>4.0.0</b>	New.
--------------	------

## set-time

Set the system time.

### Syntax

```
execute set-time <time_str>
```

The variable `<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
```

### History

<b>4.0.0</b>	New.
--------------	------

## shutdown

Use this command to shut down the FortiScan unit.

### Syntax

```
execute shutdown
```

### History

<b>4.0.0</b>	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

<b>4.0.0</b>	New.
--------------	------

## upload-benchmark

Use this command to upload benchmarks to the FortiScan Appliance.

### Syntax

```
execute upload_benchmark {[ftp | sftp | scp | tftp] <address_ipv4>
  <arg_1> <arg_2> <arg_3> <arg_4>}
```

Keywords and variables	Description
<pre>upload_benchmark {[ftp   sftp   scp   tftp] &lt;address_ipv4&gt; &lt;arg_1&gt; &lt;arg_2&gt; &lt;arg_3&gt; &lt;arg_4&gt;}</pre>	<p>Upload a benchmark from a file on a FTP, SFTP, SCP, or TFTP server, where:</p> <ul style="list-style-type: none"> <li>• &lt;address_ipv4&gt; - The IP address of the server where the backup file is located.</li> <li>• &lt;arg_1&gt; - For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename.</li> <li>• &lt;arg_2&gt; - For FTP, SFTP or SCP enter a password or enter '.'. For TFTP enter the filename or press Enter.</li> <li>• &lt;arg_3&gt; - For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter.</li> <li>• &lt;arg_4&gt; - Enter a filename or press Enter.</li> </ul> <p><b>Note:</b> Use the FTP server's IP address whenever you are entering the FTP server information. Using a domain name is not supported.</p>

### Example

The command in the following example upload the benchmark file FDCC-Major-Version-1.2.x.0-12172009-1831.zip from the FTP server at IP address 172.17.94.96.

```
execute upload-benchmark ftp 172.17.94.96 henrydu - ./ FDCC-
Major-Version-1.2.x.0-12172009-1831.zip
```

### History

**4.0.0** 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>
execute vm update-fds
execute vm update-manual <service [ftp | sftp | scp | tftp]>
execute vm update-status-list
execute vm update-refresh
```

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.
update-fds	Immediately update the Vulnerability Management packages through the FortiGuard network. This takes a few minutes.
update-manual <service [ftp   sftp   scp   tftp]>	Enter to manually update the vulnerability management package.
update-status-list	Enter to list the status of the update.
update-refresh	Enter to refresh the FortiGuard network status.

### Example

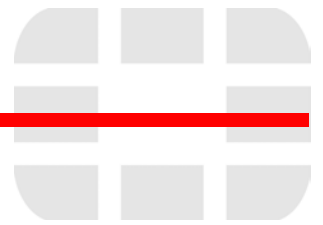
The following example shows how to schedule when updates for vulnerabilities should occur.

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

## History

4.0.0

New.



# get

`get` commands display a part of your FortiScan unit's configuration in the form of a list of settings and their values.



**Note:** Although not explicitly shown in this section, for all `config` commands, there are related `show` and `get` 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 `show`, `get` displays **all** settings, even if they are still in their default state.

For example, you might get the current DNS settings:

```
FortiScan-3000C# 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.

Most `get` commands, such as `get system dns`, are used to display configured settings. You can find relevant information about such commands in the corresponding `config` 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](#)

## system performance

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

### Syntax

```
get system performance
```

### Example

This example shows typical results returned by a FortiScan-3000C Appliance in response to the following command:

```
FortiScan-3000C # get system performance
```

Output:

```
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 minutes
CPU usage:     0% used,
100% idle
```

### History

<b>4.0.0</b>	New.
--------------	------

### Related topics

- [get system status](#)

## system status

Use this command to display FortiScan system status information including:

- firmware version, build number and date
- branching point (same as firmware build number)
- release version
- FortiScan unit serial number and BIOS version
- vulnerability management engine and plug-in version
- number of registered host asset IP addresses
- maximum number of host asset IP addresses allowed
- hostname
- FIPS mode status
- system time
- disk usage

### Syntax

```
get system status
```

### Example

This example shows typical results returned by a FortiScan-3000C Appliance in response to the following command:

```
FortiScan-3000C # get system status
```

Output:

```
Version: FortiScan-3000C v4.0,build0152,100514 (Interim)
Branch point: 140
Release Version Information: Interim
Serial-Number: FSC3KC3R10600008
BIOS version: 00010017
VCM Service Pack: 2.016_1.118 [Wed May 12 12:10:00 2010]
Registered Compliance Host Asset IP Addresses: 5995
Max Number of Compliance Host Asset IP Addresses: 6000
Registered Compliance Host Asset Agents: 5994
Max Number of Compliance Host Asset Agents: 6000
Hostname: FortiScan-3000C
FIPS mode: disabled
System Time: Mon May 17 11:02:08 PDT 2010

Disk Usage: Free 1612.50GB, Total 1832.78GB
RAID information:
RAID level: RAID0
RAID state: OK
RAID controller: PERC 6/i Integrated
Number of disks: 2
Array capacity: 1862.00GB

Disk      State      Size
disk01   OK         931.51GB
disk02   OK         931.51GB
```

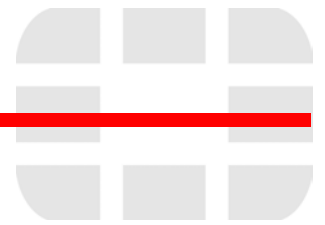
```
disk03 NotPresent
disk04 NotPresent
disk05 NotPresent
disk06 NotPresent
```

## History

```
4.0.0 New.
```

## Related topics

- [get system performance](#)



# diagnose

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

This chapter contains the following sections:

<a href="#">alertmail</a>	<a href="#">debug emserver</a>	<a href="#">gui</a>
<a href="#">cmdb</a>	<a href="#">debug info</a>	<a href="#">netlink</a>
<a href="#">debug application</a>	<a href="#">debug output</a>	<a href="#">ntpd</a>
<a href="#">debug capture-output</a>	<a href="#">debug report</a>	<a href="#">raid</a>
<a href="#">debug cli</a>	<a href="#">debug reset</a>	<a href="#">sniffer</a>
<a href="#">debug crashlog</a>	<a href="#">debug timestamp</a>	<a href="#">sys</a>
<a href="#">debug emdb</a>	<a href="#">fortiguard</a>	<a href="#">vm</a>

## 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 at IP address <ftp_host_IP>.

### 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

4.0.0	New.
-------	------

## cldb

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

### Syntax

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

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

### Example

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

```
diagnose cldb error-msg upload 192.168.10.1
```

### History

**4.0.0**            New.

## debug application

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

### Syntax

```
diagnose debug application alert <debug_level_integer>
diagnose debug application alertmail <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 miglogd <debug_level_integer>
diagnose debug application network-summary <debug_level_integer>
diagnose debug application ntpd <debug_level_integer>
diagnose debug application remote-auth <debug_level_integer>
diagnose debug application snmpd <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
cmdb <debug_level_integer>	Set the debug level of FortiScan 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
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
remote-auth <debug_level_integer>	Set the debug level of the remote authentication daemon from 0-8.	0
snmpd <debug_level_integer>	Set the debug level of the SNMP 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

<b>4.0.0</b>	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

**4.0.0**            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

**4.0.0**            New.

## debug crashlog

Use this command to manage crash logs.

### Syntax

```
diagnose debug crashlog clear
diagnose debug crashlog get <alertmail | auto-rm-files | cmdbsvr |
  cmf | fdpd | flgdns | fnbamd | httpsd | hwmond | klogd | miglogd
  | newcli | ntpd | smit | sniffd | snmpd | uploadd | vmagent |
  vmpdated>
diagnose debug crashlog list
diagnose debug crashlog upload <alertmail | auto-rm-files |
  cmdbsvr | cmf | fdpd | flgdns | fnbamd | httpsd | hwmond | klogd
  | miglogd | newcli | ntpd | smit | sniffd | snmpd | uploadd |
  vmagent | vmpdated>
```

Variable	Description
clear	Delete backtrace and core files.
get <alertmail   auto-rm-files   cmdbsvr   cmf   fdpd   flgdns   fnbamd   httpsd   hwmond   klogd   miglogd   newcli   ntpd   smit   sniffd   snmpd   uploadd   vmagent   vmpdated>	Display the backtrace for an application.
list	List applications that have backtraces or core files.
upload <alertmail   auto-rm-files   cmdbsvr   cmf   fdpd   flgdns   fnbamd   httpsd   hwmond   klogd   miglogd   newcli   ntpd   smit   sniffd   snmpd   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:

```
FortiScan-3000C # diagnose debug crashlog 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

4.0.0                      New.

## debug emdb

Use this command to view FortiScan DB logs.

### Syntax

```
diagnose debug emdb listlogs
diagnose debug emdb loghist <yyyy-mm-dd>
diagnose debug emdb logrt <log_file name>
diagnose debug emdb readlog <log_file name>
diagnose debug emdb upload {[ftp | sftp | scp | tftp]
  <address_ipv4> <arg_1> <arg_2> <arg_3> <arg_4>}
```

Variable	Description
listlogs	List all available logs. The name is useful for logrt command.
loghist <yyyy-mm-dd>	Print out all logs which time stamp is specified.
logrt <log_file name>	Monitor logs real time.
readlog <log_file name>	Open one log and print out on the screen.
upload {[ftp   sftp   scp   tftp] <address_ipv4> <arg_1> <arg_2> <arg_3> <arg_4>}	Upload one log to an FTP, SFTP, SCP, or TFTP server, where: <ul style="list-style-type: none"> <li>• &lt;address_ipv4&gt; – The IP address of the server.</li> <li>• &lt;arg_1&gt; – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename.</li> <li>• &lt;arg_2&gt; – For FTP, SFTP or SCP enter a password or enter ‘.’. For TFTP enter the filename or press Enter.</li> <li>• &lt;arg_3&gt; – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter.</li> <li>• &lt;arg_4&gt; – Enter a filename or press Enter.</li> </ul> <b>Note:</b> Use the FTP server’s IP address whenever you are entering the FTP server information. Using a domain name is not supported.

### Example

This example shows how to list emdb logs:

```
FortiScan-3000C # diagnose debug emdb listlogs
```

Output:

```
dblog.tgz: 25030 bytes, Mon May 17 13:33:04 PDT 2010
postgresql-2010-05-09_215509.log: 3743 bytes, Sun May 9
  15:07:28 PDT 2010
postgresql-2010-05-10_000000.log: 160307 bytes, Mon May 10
  10:35:10 PDT 2010
postgresql-2010-05-10_173800.log: 2247 bytes, Mon May 10
  14:12:09 PDT 2010
postgresql-2010-05-10_211457.log: 1081 bytes, Mon May 10
  14:48:42 PDT 2010
postgresql-2010-05-10_215130.log: 150 bytes, Mon May 10 14:51:31
  PDT 2010
postgresql-2010-05-11_000000.log: 1309 bytes, Tue May 11
  09:31:03 PDT 2010
postgresql-2010-05-11_163353.log: 150 bytes, Tue May 11 09:33:53
  PDT 2010
```

```
postgresql-2010-05-12_000000.log: 2789 bytes, Wed May 12  
09:16:29 PDT 2010  
postgresql-2010-05-12_162632.log: 2344 bytes, Wed May 12  
16:46:23 PDT 2010
```

## History

**4.0.0**            New.

## debug emserver

Use this command to view all FortiScan EM Server logs.

### Syntax

```
diagnose debug emserver listlogs
diagnose debug emserver loghist <yyyy-mm-dd>
diagnose debug emserver logrt <log_file name>
diagnose debug emserver readlog <log_file name>
diagnose debug emserver upload {[ftp | sftp | scp | tftp]
  <address_ipv4> <arg_1> <arg_2> <arg_3> <arg_4>}
```

Variable	Description
listlogs	List all available logs. The name is useful for logrt command.
loghist <yyyy-mm-dd>	Print out all logs which time stamp is specified.
logrt <log_file name>	Monitor logs real time.
readlog <log_file name>	Open one log and print out on the screen.
upload {[ftp   sftp   scp   tftp] <address_ipv4> <arg_1> <arg_2> <arg_3> <arg_4>}	<p>Upload one log to an FTP, SFTP, SCP, or TFTP server, where:</p> <ul style="list-style-type: none"> <li>• &lt;address_ipv4&gt; – The server IP address</li> <li>• &lt;arg_1&gt; – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename.</li> <li>• &lt;arg_2&gt; – For FTP, SFTP or SCP enter a password or enter ‘.’. For TFTP enter the filename or press Enter.</li> <li>• &lt;arg_3&gt; – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter.</li> <li>• &lt;arg_4&gt; – Enter a filename or press Enter.</li> </ul> <p><b>Note:</b> Use the FTP server’s IP address whenever you are entering the FTP server information. Using a domain name is not supported.</p>

### Example

This example shows how to list FortiScan EM Server logs:

```
FortiScan-3000C # diagnose debug emserver listlogs
```

Output:

```
em.log: 8995221 bytes, Mon May 17 13:43:04 PDT 2010
em.log.1: 52428926 bytes, Mon May 17 13:32:47 PDT 2010
em.log.10: 52428910 bytes, Mon May 17 05:49:19 PDT 2010
em.log.2: 52428971 bytes, Mon May 17 12:12:33 PDT 2010
em.log.3: 52428883 bytes, Mon May 17 10:49:34 PDT 2010
em.log.4: 52429235 bytes, Mon May 17 09:42:39 PDT 2010
em.log.5: 52428805 bytes, Mon May 17 08:54:32 PDT 2010
em.log.6: 52428881 bytes, Mon May 17 08:03:49 PDT 2010
em.log.7: 52428906 bytes, Mon May 17 07:34:55 PDT 2010
em.log.8: 52429040 bytes, Mon May 17 06:57:31 PDT 2010
em.log.9: 52428836 bytes, Mon May 17 06:18:40 PDT 2010
```

## History

4.0.0

New.

## debug info

Use this command to show active debug level settings.

### Syntax

```
diagnose debug info
```

### History

<b>4.0.0</b>	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

**4.0.0**            New.

## debug report

Use this command to display FortiScan configuration.

### Syntax

```
diagnose debug report
```

### History

<b>4.0.0</b>	New.
--------------	------

## debug reset

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

### Syntax

```
diagnose debug reset
```

### History

<b>4.0.0</b>	New.
--------------	------

## debug timestamp

Use this command to enable or disable debug timestamp.

### Syntax

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

### History

<b>4.0.0</b>	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

**4.0.0**      New.

## gui

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

### Syntax

```
diagnose gui console
```

### History

<b>4.0.0</b>	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 FortiScan unit's interface statistics.
interface list	Display the FortiScan unit's interface status and parameters.
ip list	Display all of the physical and virtual IP addresses associated with the network interfaces of the FortiScan unit.
route list	Display the FortiScan unit's routing table contents.
rtcache list	Display the FortiScan unit's routing cache information.
tcp list	Display the FortiScan unit's TCP socket information.
udp list	Display the FortiScan unit's UDP sockets information.

### Example

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

```
FortiScan-3000C # 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=tun10 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

4.0.0

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 at IP address <ftp_host_ip>.

### Example

This example shows how to list the NTPD error messages:

```
FortiScan-3000C # 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

**4.0.0**                      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 FortiScan-3000C Appliance:

```
FortiScan-3000C # diagnose raid info
```

Output:

```
Free Disk Space: 1612.49GB
Total Disk Space: 1832.78GB
```

```
RAID information:
RAID level: RAID0
RAID state: OK
RAID controller: PERC 6/i Integrated
Number of disks: 2
Array capacity: 1862.00GB
```

```
Disk   State   Size
disk01 OK       931.51GB
disk02 OK       931.51GB
disk03 NotPresent
disk04 NotPresent
disk05 NotPresent
disk06 NotPresent
```

Controller configuration:

```
Adapter 0 -- Virtual Drive Information:
Virtual Disk: 0 (Target Id: 0)
Name:
RAID Level: Primary-0, Secondary-0, RAID Level Qualifier-0
Size:1906688MB
State: Optimal
Stripe Size: 64kB
Number Of Drives:2
Span Depth:1
Default Cache Policy: WriteBack, ReadAheadNone, Direct, No Write
Cache if Bad BBU
Current Cache Policy: WriteBack, ReadAheadNone, Direct, No Write
Cache if Bad BBU
Access Policy: Read/Write
```

```
Disk Cache Policy: Disk's Default

Disk layout:

Adapter #0

Number of Virtual Disks: 1
Virtual Disk: 0 (Target Id: 0)
Name:
RAID Level: Primary-0, Secondary-0, RAID Level Qualifier-0
Size:1906688MB
State: Optimal
Stripe Size: 64kB
Number Of Drives:2
Span Depth:1
Default Cache Policy: WriteBack, ReadAheadNone, Direct, No Write
    Cache if Bad BBU
Current Cache Policy: WriteBack, ReadAheadNone, Direct, No Write
    Cache if Bad BBU
Access Policy: Read/Write
Disk Cache Policy: Disk's Default
Number of Spans: 1
Span: 0 - Number of PDs: 2
PD: 0 Information
Enclosure Device ID: 32
Slot Number: 0
Device Id: 0
Sequence Number: 2
Media Error Count: 0
Other Error Count: 0
Predictive Failure Count: 0
Last Predictive Failure Event Seq Number: 0
PD Type: SATA
Raw Size: 953869MB [0x74706db0 Sectors]
Non Coerced Size: 953357MB [0x74606db0 Sectors]
Coerced Size: 953344MB [0x74600000 Sectors]
Firmware state: Online
SAS Address(0): 0x1221000000000000
Connected Port Number: 0(path0)
Inquiry Data: ATA      WDC WD1002FBYS-10C06      WD-WMATV2807038
Foreign State: None
Media Type: Hard Disk Device

PD: 1 Information
Enclosure Device ID: 32
Slot Number: 1
Device Id: 1
Sequence Number: 2
Media Error Count: 0
Other Error Count: 0
Predictive Failure Count: 0
Last Predictive Failure Event Seq Number: 0
PD Type: SATA
Raw Size: 953869MB [0x74706db0 Sectors]
```

```
Non Coerced Size: 953357MB [0x74606db0 Sectors]
Coerced Size: 953344MB [0x74600000 Sectors]
Firmware state: Online
SAS Address(0): 0x1221000001000000
Connected Port Number: 1(path0)
Inquiry Data: ATA      WDC WD1002FBYS-10C06      WD-WMATV2820089
Foreign State: None
Media Type: Hard Disk Device
```

## History

4.0.0            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.

FortiScan units have a built-in sniffer. Packet capture on FortiScan 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 FortiScan 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 <code>port1</code> , or type <code>any</code> to capture packets on all network interfaces.
'<filter_str>'	Type either <code>none</code> 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 <code>'tcp port 25'</code> . Surround the filter string in quotes. The filter uses the following syntax: <code>'[[src dst] host {&lt;host1_fqdn&gt;   &lt;host1_ip4&gt;}] [and or] [[src dst] host {&lt;host2_fqdn&gt;   &lt;host2_ip4&gt;}] [and or] [[arp ip gre esp udp tcp] port &lt;port1_int&gt;] [and or] [[arp ip gre esp udp tcp] port &lt;port2_int&gt;]'</code> 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 <code>1.example.com</code> and either <code>2.example.com</code> or <code>3.example.com</code> , you would enter: <code>'udp and port 1812 and src host 1.example.com and dst \ ( 2.example.com or 2.example.com \)'</code>
{1   2   3}	Type one of the following integers indicating the depth of packet headers and payloads to capture: <ul style="list-style-type: none"> <li>1 for header only</li> <li>2 for IP header and payload</li> <li>3 for Ethernet header and payload</li> </ul> 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).

```
FortiScan-3000C # 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 FortiScan unit are not bolded.

```
FortiScan-3000C # 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 FortiScan unit are not bolded.

```
FortiScan-3000C # 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 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\FortiScan\_sniff.txt.
- 4 Press Enter to send the CLI command to the FortiScan 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 FortiScan_sniff.txt -out FortiScan_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
- `FortiScan_sniff.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `FortiScan_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**

```

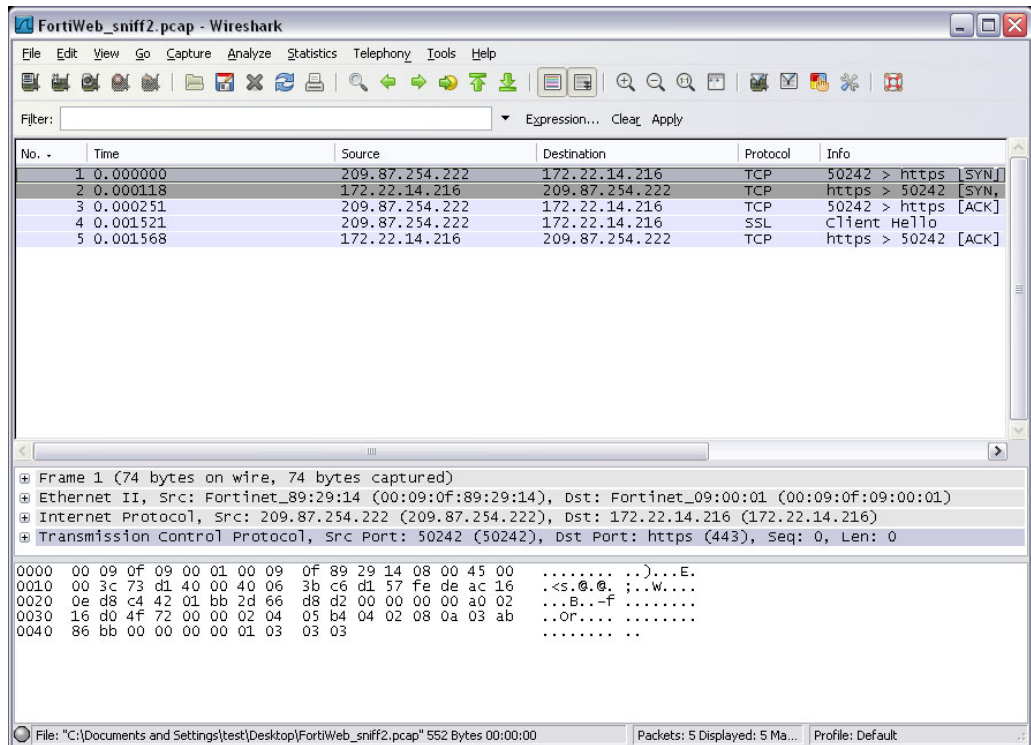
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\test>cd Desktop
C:\Documents and Settings\test\Desktop>fgt2eth.pl -in FortiWeb_sniff.txt -out FortiWeb_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)
Output 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



For additional information on packet capture, see the Fortinet Knowledge Base article [Using the FortiOS built-in packet sniffer](#).

## History

**4.0.0**                      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 FortiScan unit and each of the registered devices.

Variable	Description
file-system {fscheck   fsfix   fsrebuild   fsreport   reset-mount-count}	<p>fscheck - Check the log disk consistency by rebooting the system. You can view the results using <code>diagnose file-system fsreport</code> after the reboot.</p> <p>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 <code>diagnose file-system fsreport</code> after the reboot.</p> <p>fsrebuild - Rebuild file system from scratches upon system reboot. This action may cause potential data loss. Do not perform this action unless the <code>fsfix</code> report has errors. You can view the results using <code>diagnose file-system fsreport</code> after the reboot.</p> <p>fsreport - Display the results of the <code>fscheck</code>, <code>fsfix</code>, and <code>fsrebuild</code> commands.</p> <p>reset-mount-count - Set the mount-count of log disk to 1 upon system reboot.</p>
fssystem	Display the log disk file system information.
interface <port>	Display the detailed information for an interface.
kill <signal> <pid>	<p>Send a signal to terminate a process that is currently running on the system.</p> <ul style="list-style-type: none"> <li>• &lt;signal&gt; - the signal number to send.</li> <li>• &lt;pid&gt; - the process ID where the signal is sent to.</li> </ul>
pciconfig	Display PCI information.
sysinfo {cpu   diskused   interrupts   iomem   ioports   memory   slab}	<p>cpu - Display detailed information for all installed CPU(s).</p> <p>diskused - Display the used space and total space of the hard disk.</p> <p>interrupts - Display system interrupts information.</p> <p>iomem - Display the memory map of I/O ports.</p> <p>ioports - Display the address list of I/O ports.</p> <p>memory - Display system memory information.</p> <p>slab - Display memory allocation information.</p>
top <value>	<p>Display the top processes.</p> <ul style="list-style-type: none"> <li>• &lt;value&gt; - the refreshing interval in seconds. The default is 5.</li> </ul>

## Example

This example shows how to display the interface information of port1:

```
FortiScan-3000C # dia sys interface port1
```

Output:

```
Interface name          port1
Link encap              Ethernet
HWaddr                  00:26:B9:61:F0:A0
inet addr                172.17.93.176
Bcast                   172.17.93.255
Mask                     255.255.255.0
Status                   up
MTU                      1500
Metric                  1
RX packets               112340
errors                   0
droppet                  0
overruns                 0
frame                   0
TX packets               92825
```

```

errors 0
droppet 0
overruns 0
carrier 0
collisions 0
txqueuelen 1000
RX bytes 19766388 (18.8M Bytes)
TX bytes 33952357 (32.3M Bytes)
Interrupt 19
Memory d6000000-d6012800
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 1
Transceiver internal
Auto-negotiation on

```

## History

**4.0.0**      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

<b>4.0.0</b>	New.
--------------	------

## vpn

Use this command to list the information about the FortiScan IPSec gateway and the VPN tunnel between a device and the FortiScan unit.

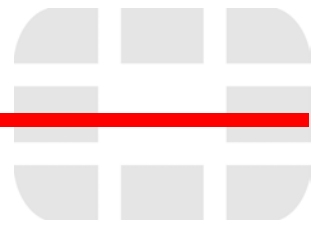
### Syntax

```
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 FortiScan IPSec gateway used for the VPN tunnel between a device and the FortiScan unit.
list	Display the information of the VPN tunnel between a device and the FortiScan unit.

### History

**4.0.0**            New.



# show

The `show` commands display a part of your FortiScan 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.

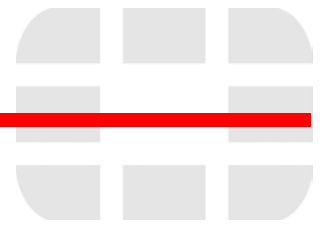
For example, you might show the current DNS settings:

```
FortiScan-3000C # 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.





# Index

## Symbols

- \_email, 16
- \_fqdn, 16
- \_index, 16
- \_int, 16
- \_ipv4, 16
- \_ipv4/mask, 16
- \_ipv4mask, 16
- \_ipv4range, 16
- \_name, 16
- \_pattern, 16
- \_str, 16
- \_url, 16
- \_v4mask, 16

## A

- abort, 18

## C

- certification, 7
- CIDR, 16
- command
  - interactive, 19
- command indentations, 15
- command notations, 16
- command syntax terminology, 14
- comments
  - , 8
- config
  - gui, 21
- connecting to the console, 12
- conventions, 8
- CPU status, 76
- CPU usage, 76
- customer service, 7

## D

- data-size, 62
- delete, shell command, 18
- df-bit, 62

## diagnose

- alertmail, 79
- cmdb, 80
- debug application, 81
- debug capture-output, 83
- debug cli, 84
- debug crashlog, 85
- debug emdb, 86, 88
- debug info, 90
- debug output, 91
- debug report, 92
- debug reset, 93
- debug timestamp, 94
- fortiguard, 95
- gui, 96
- netlink, 97
- ntpd, 99
- raid, 100
- sys, 108
- vm, 111
- vpn, 112

- Diagnose commands, 10

- documentation, 8
  - commenting on, 8
  - conventions, 8
  - Fortinet, 8

- dotted decimal, 16

## E

- edit
  - shell command, 18
- enabling access to cli
  - ssh, 13
  - telnet, 13
- end
  - command in an edit shell, 18
  - shell command, 18
- execute
  - backup, 54
  - disconnect, 55
  - factoryreset, 60
  - ping, 61
  - ping-options, 62
  - reboot, 64
  - reload, 65
  - restore, 66
  - set-date, 68
  - set-time, 69
  - shutdown, 70
  - update-vm, 72
  - vm, 73
- execute command
  - ping, 61, 71
  - restore, 71

**F**

factoryreset, execute, 60  
 FAQ, 8  
 FortiGuard  
   Antivirus, 7  
   services, 7  
 Fortinet  
   Knowledge Base, 8  
   Knowledge Center, 8  
   Technical Documentation, 8  
     conventions, 8  
   Technical Support, 7, 103  
   Technical Support, registering with, 7  
   Technical Support, web site, 7  
   Training Services, 7  
 Fortinet customer service, 7  
 Fortinet documentation, 8  
 fully qualified domain name (FQDN), 16

**G**

get  
   edit shell command, 18  
   shell command, 18  
 glossary, 8

**H**

how-to, 8

**I**

image, 66  
 index number, 16  
 introduction  
   Fortinet documentation, 8  
 IP address  
   private network, 8

**K**

Knowledge Center, 8

**M**

memory usage, 76

**N**

next, 18

**P**

packet  
   capture, 103  
   trace, 103  
 pattern, 16  
 pattern, ping-options, 62  
 ping, execute, 61, 71  
 ping-options, execute, 62  
 product registration, 7  
 purge, shell command, 18

**R**

registering  
   with Fortinet Technical Support, 7  
 regular expression, 16  
 rename, shell command, 18  
 repeat-count, 62  
 report  
   output, 22  
 restore, execute, 66, 71  
 RFC  
   1918, 8

**S**

set, 18  
 shell command  
   delete, 18  
   edit, 18  
   end, 18  
   get, 18  
   purge, 18  
   rename, 18  
   show, 18  
 show, 18  
 show, shell command, 18  
 sniffer, 103  
 source, ping-options, 62  
 string, 16  
 system  
   console, 24  
   dns, 25  
   fips, 26  
   fortiguard, 27  
   global, 29  
   interface, 30  
   mail, 32  
   ntp, 33  
   raid, 34  
   route, 35  
   snmp, 36

**T**

technical  
   documentation, 8  
   documentation conventions, 8  
   notes, 8  
   support, 7  
 technical support, 7  
 timeout, ping-options, 62  
 tips and tricks  
   abbreviations for commands, 19  
   shortcuts, keyboard commands, 19  
   special characters, 19  
   supported languages, 20  
   viewing help, 19  
 tos, 62  
 Training Services, 7  
 troubleshooting, 9, 79, 103  
 ttl, 62

## U

uniform resource identifier (URI), 16  
uniform resource locator (URL), 16  
unset, 18  
up time, 76  
US-ASCII, 105

## V

validate-reply, 62  
value parse error, 16  
view-settings, 62

## W

wild cards, 16



**F**ORTINET®

[www.fortinet.com](http://www.fortinet.com)

**F**ORTINET®

[www.fortinet.com](http://www.fortinet.com)