



FortiScan™

Version 4.0 MR2 Patch 3
CLI Reference

FortiScan Version 4.0 MR2 Patch 3 CLI Reference

Revision 1

27 October 2011

© Copyright 2011 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

ABACAS, APSecure, Dynamic Threat Prevention System (DTPS), FortiAnalyzer®, FortiASIC, FortiBIOS, FortiBridge, FortiClient®, FortiDB, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiMail®, FortiManager®, Fortinet®, FortiOS®, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiScan, FortiShield, FortiVoIP, FortiWeb, FortiWiFi, and TalkSwitch® 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.

Contents

Introduction	11
Registering your FortiScan appliance	11
Customer service & technical support	11
Training	12
Documentation	12
Fortinet Tools and Documentation CD	12
Fortinet Knowledge Base	12
Comments on Fortinet technical documentation	12
Scope	12
Conventions	13
IP addresses	13
Cautions, notes, & tips	13
Typographical conventions	13
Command syntax conventions	14
What's new	15
Structure changes.....	15
FortiScan-VM	15
Using the CLI	17
Connecting to the CLI.....	17
Connecting to the CLI using a local console.....	18
Enabling access to the CLI through the network (SSH or Telnet or CLI Console widget)	19
Connecting to the CLI using SSH.....	20
Connecting to the CLI using Telnet	21
Command syntax	22
Terminology	22
Indentation	23
Notation	23
Sub-commands	24
Table commands	26
Example of table commands	26
Field commands	27
Example of field commands	27

Tips and tricks	27
Help	28
Shortcuts and key commands	28
Command abbreviation.....	28
Special characters	28
Language support.....	29
Screen paging.....	30
Baud rate	30
Editing the configuration file on an external host	30
config global	33
gui console	34
Syntax.....	34
Related topics	34
system console	35
Syntax.....	35
Example.....	35
Related topics	35
system dns	36
Syntax.....	36
Example.....	36
Related topics	36
system fortiguard	37
Syntax.....	37
Example.....	38
Related topics	38
system global	39
Syntax.....	39
Example.....	39
Related topics	39
system interface	40
Syntax.....	40
Example.....	41
Related topics	41
system mail	42
Syntax.....	42
Example.....	42
Related topics	42
system ntp	43
Syntax.....	43
Example.....	43
Related topics	43

system raid	44
Syntax	44
Example	44
Related topics	44
system route	45
Syntax	45
Example	45
Related topics	45
system snmp	46
Syntax	46
Example	47
Related topics	48
config adom	49
report output	50
Syntax	50
Example	51
Related topics	51
system mail	52
Syntax	52
Example	52
Related topics	52
vm map-config	53
Syntax	53
Example	54
Related topics	55
vm scan-profile	56
Syntax	56
Example	56
Related topics	57
vm schedule	58
Syntax	58
Example	59
Related topics	59
vm sensor	60
Syntax	60
Example	62
Related topics	62
execute	63
backup config	64
Syntax	64
Example	64
Related topics	65

backup config-secure	66
Syntax	66
Example	66
Related topics	67
disconnect	68
Syntax	68
Example	68
Example	68
em_dbbackup	69
Syntax	69
Example	69
Related topics	70
em_dbrestore	71
Syntax	71
Example	71
Related topics	72
factoryreset	73
Syntax	73
Related topics	73
ping	74
Syntax	74
Example	74
Related topics	74
ping-options	75
Syntax	75
Example	75
Example	75
Related topics	76
reboot	77
Syntax	77
Related topics	77
reload	78
Syntax	78
Related topics	78
remove	79
Syntax	79
reset_password	80
Syntax	80
restore config	81
Syntax	81
Related topics	81

restore config-secure	82
Syntax.....	82
Related topics	82
restore image.....	83
Syntax.....	83
Related topics	83
restore vm.....	84
Syntax.....	84
Related topics	84
set-date	85
Syntax.....	85
Example.....	85
Related topics	85
set-time	86
Syntax.....	86
Example.....	86
Related topics	86
shutdown	87
Syntax.....	87
Related topics	87
traceroute.....	88
Syntax.....	88
Related topics	88
upload-benchmark.....	89
Syntax.....	89
Example.....	89
vm	90
Syntax.....	90
Example.....	90
Related topics	90
get.....	93
system performance	94
Syntax.....	94
Example.....	94
Related topics	94
system status	95
Syntax.....	95
Example.....	95
Related topics	96

diagnose	97
alertmail error-msg	98
Syntax.....	98
Example.....	98
Related topics	98
cmdb	99
Syntax.....	99
Example.....	99
Related topics	99
debug application	100
Syntax.....	100
Example.....	100
Related topics	101
debug capture-output	102
Syntax.....	102
Example.....	102
debug cli	103
Syntax.....	103
Example.....	103
Related topics	103
debug crashlog	104
Syntax.....	104
Example.....	104
Related topics	105
debug dbsync	106
Syntax.....	106
Example.....	106
Related topics	107
debug emdb	108
Syntax.....	108
Example.....	108
Related topics	108
debug emserver	109
Syntax.....	109
Example.....	109
Related topics	110
debug info	111
Syntax.....	111
debug output	112
Syntax.....	112
Example.....	112
Related topics	112

debug report	113
Syntax	113
debug reset	114
Syntax	114
Related topics	114
debug timestamp	115
Syntax	115
Related topics	115
fortiguard	116
Syntax	116
Example	116
Related topics	116
gui console	117
Syntax	117
Related topics	117
netlink	118
Syntax	118
Example	118
Related topics	119
ntpd	120
Syntax	120
Example	120
Related topics	120
raid	121
Syntax	121
Example	121
Related topics	123
sniffer packet	124
Syntax	124
Example	125
Example	125
Example	125
Related topics	129
sys	130
Syntax	130
Example	131
Related topics	132
vm downgrade	133
Syntax	133
Example	133
Related topics	133

vm engine-log	134
Syntax.....	134
Related topics	134
vm error-msg clear	135
Syntax.....	135
Related topics	135
vm error-msg show	136
Syntax.....	136
Example.....	136
Related topics	136
vm error-msg upload	137
Syntax.....	137
Example.....	137
Related topics	137
vm status	138
Syntax.....	138
Example.....	138
Related topics	138
show	139
Index	141

Introduction

Welcome, and thank you for selecting Fortinet products for your network protection.

The FortiScan Vulnerability and Compliance Management (VCM) platform is a managed security service provider (MSSP)- and enterprise-level IT security solution that empowers you to protect your many network hosts from known vulnerabilities and exploits.

FortiScan network appliances, together with FortiScan agents, help you to efficiently address the ever-increasing number of computer security threats. FortiScan network appliances provide ready-to-deploy remediation actions and enforcement actions, which can change host configurations to mitigate weak settings and patch applications. This frees your time to focus on zero-day vulnerabilities and exploits, before vendor-provided patches or fixes are available.

FortiScan network appliances can also scan your network for vulnerabilities and compliance exposures, prioritizing hosts by risk.

This topic includes:

- [Registering your FortiScan](#)
- [Forums](#)
- [Technical support](#)
- [Training](#)
- [Documentation](#)
- [Scope](#)
- [Conventions](#)

Registering your FortiScan

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 services require product registration.

For more information, see the Fortinet Knowledge Base article [Registration Frequently Asked Questions](#).

Forums

Fortinet Technical Discussion forums provide a place for you to connect with your fellow IT professionals to discuss best practices and solutions. Visit the forums at:

<http://support.fortinet.com/forum/>

Technical support

Fortinet Technical Support provides services designed to make sure that you can install your Fortinet products quickly, configure them easily, and operate them 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 [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://training.fortinet.com>

or e-mail them at:

training@fortinet.com

Documentation

The Fortinet Technical Documentation web site:

<http://docs.fortinet.com>

provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

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

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD that ships with physical Fortinet appliances. 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, and FAQs. 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 document to:

techdoc@fortinet.com

Scope

This document describes how to use the command line interface (CLI) of the FortiScan appliance. It assumes that you have already successfully installed the FortiScan appliance and completed basic setup by following the instructions in the *FortiScan Install Guide*.

At this stage:

- You have administrative access to the web UI and/or CLI.
- The FortiScan appliance is integrated into your network.
- The FortiScan agent has been installed on hosts that you want to monitor and/or manage.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware and FortiGuard Vulnerability Management Service (VCM) plug-in and engine updates have been completed.

Once that basic installation is complete, you can use this document. This document explains how to use the CLI to:

- Maintain the FortiScan appliance, including backups.
- Reconfigure basic items that were configured during installation.
- Configure advanced features, such as asset management, compliance management, vulnerability management, remediation, logging, and reporting.

This document does **not** cover the web UI. For information on the web UI, see the *FortiScan Administration Guide*.

This document is intended for administrators, not end users. If you have a user account on a host where the FortiScan agent is installed, please contact your system administrator.

Conventions

Fortinet technical documentation uses the conventions described below.

IP addresses

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

<http://ietf.org/rfc/rfc1918.txt?number-1918>

Cautions, notes, & tips

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



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



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



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

Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 1: Typographical conventions in Fortinet technical documentation

Convention	Example
Button, menu, text box, field, or check box label	From <i>Minimum log level</i> , select <i>Notification</i> .
CLI input	<pre>config system dns set primary <address_ipv4> end</pre>
CLI output	<pre>FGT-602803030703 # get system settings comments : (null) opmode : nat</pre>
Emphasis	HTTP connections are <i>not</i> secure and can be intercepted by a third party.
File content	<pre><HTML><HEAD><TITLE>Firewall Authentication</TITLE></HEAD> <BODY><H4>You must authenticate to use this service.</H4></pre>
Hyperlink	Visit the Fortinet Technical Support web site, https://support.fortinet.com .
Keyboard entry	Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code> .
Navigation	Go to <code>VPN > IPSEC > Auto Key (IKE)</code> .
Publication	For details, see the <i>FortiGate Administration Guide</i> .

Command syntax conventions

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

For command syntax conventions such as braces, brackets, and command constraints such as `<address_ipv4>`, see “[Notation](#)” on page 23.

What's new

The table below lists commands which have changed since FortiScan 4.0 MR1, including new commands, syntax changes, and new setting options.

Command	Change
<code>execute remove</code>	New command. Removes reports.
<code>execute reset_password</code>	New command. Resets the password of the admin administrator account to its default value, P@ssword1.
<code>diagnose debug dbsync</code>	New command. Displays logs relating to internal FortiScan database synchronization.
<code>get system status</code>	Changed. Support added for FortiScan-VM.

Structure changes

Due to the addition of the administrative domain (ADOM) feature, all commands are now nested within either a `config global` or `config adom` command.

- Global commands affect system-wide settings and are thus available under `config global`. These include `diagnose` commands, `execute` commands, and some `config` commands that affect system-wide features such as the web UI and network interfaces. The syntax for modifying global settings is:

```
config global
  config ...
  diagnose ...
  execute ...
end
```

- ADOM commands affect ADOM-wide settings and are thus available under `config adom`. These include `config` commands that affect asset data such as report settings and vulnerability management settings. The syntax for modifying settings specific to an ADOM is:

```
config adom
  edit <adom_name>
    config ...
    execute vm ...
  end
end
```

For more information about ADOMs, see the [FortiScan Administration Guide](#) or the online help.

FortiScan-VM

FortiScan is now available as a virtual appliance that can be deployed in virtual machine environments such as VMware vSphere and Citrix XenServer. For VM-specific installation instructions, see the [FortiScan-VM Install Guide](#). See also “`get system status`” on page 95.

Using the CLI

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

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

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



Note: Only the `admin` administrator account can log in to the CLI.

This section contains the following topics:

- [Connecting to the CLI](#)
- [Command syntax](#)
- [Sub-commands](#)
- [Tips and tricks](#)

Connecting to the CLI

You can access the CLI in two ways:

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

Local access is required in some cases.

- If you are installing your FortiScan appliance for the first time and it is not yet configured to connect to your network, unless you reconfigure your computer's network settings for a peer connection, you may only be able to connect to the CLI using a local serial console connection. See the [FortiScan Install Guide](#).
- Restoring the firmware utilizes a boot interrupt. Network access to the CLI is not available until **after** the boot process has completed, and therefore local CLI access is the only viable option.

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

This section includes:

- [Connecting to the CLI using a local console](#)
- [Enabling access to the CLI through the network \(SSH or Telnet or CLI Console widget\)](#)
- [Connecting to the CLI using SSH](#)

- [Connecting to the CLI using Telnet](#)

Connecting to the CLI using a local console

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

Requirements

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



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

To connect to the CLI using a local serial console connection

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

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

- 4 In the *Category* tree on the left, go to *Session* (**not** the sub-node, *Logging*) and from *Connection type*, select *Serial*.
- 5 Click *Open*.
- 6 Press the Enter key to initiate a connection.
The login prompt appears.
- 7 Type `admin` then press Enter.



Note: Other administrator accounts cannot log in to the CLI of FortiScan appliances.

- 8 Type the password for that administrator account and press Enter. (In its default state, the password for the `admin` account is `P@ssword1`.)

The CLI displays the following text, followed by a command line prompt:

```
Welcome!
```

You can now enter CLI commands, including configuring access to the CLI through SSH or Telnet. For details, see [“Enabling access to the CLI through the network \(SSH or Telnet or CLI Console widget\)”](#) on page 19.

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

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



Note: If you do not want to use an SSH/Telnet client and you have access to the web UI, you can alternatively access the CLI through the network using the *CLI Console* widget in the web UI. For details, see the [FortiScan Administration Guide](#).

You must enable SSH and/or Telnet on the network interface associated with that physical network port. If your computer is **not** connected directly or through a switch, you must also configure the FortiScan appliance with a static route to a router that can forward packets from the FortiScan appliance to your computer (see “[system route](#)” on page 45).

You can do this using either:

- a local console connection (see the following procedure)
- the web UI (see the [FortiScan Install Guide](#) or the [FortiScan Administration Guide](#))

Requirements

- a computer with an available serial communications (COM) port and RJ-45 port
- terminal emulation software such as PuTTY
- the RJ-45-to-DB-9 or null modem cable included in your FortiScan package
- a crossover Ethernet cable (if connecting directly) or straight-through Ethernet cable (if connecting through a switch or router)
- prior configuration of the network interface and static route (for details, see the [FortiScan Install Guide](#))

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

- 1 Using the network cable, connect the FortiScan appliance’s network port either directly to your computer’s network port, or to a network through which your computer can reach the FortiScan appliance.
- 2 Note the number of the physical network port.
- 3 Using a local console connection, connect and log into the CLI. For details, see “[Connecting to the CLI using a local console](#)” on page 18.

4 Enter the following commands:

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

where:

- <interface_str> is the name of the network interface associated with the physical network port, such as port1
- {aggregator http https ping ssh telnet webservice} is the complete, space-delimited list of permitted administrative access protocols, such as https ssh telnet; omit protocols that you do not want to permit

For example, to exclude HTTP, HTTPS, SNMP, and PING, and allow only SSH and Telnet administrative access on port1:

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

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



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

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

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

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

6 If you will be connecting indirectly, through one or more routers or firewalls, configure the appliance with at least one static route so that replies from the CLI can reach your client. See [“system route” on page 45](#).

To connect to the CLI through the network interface, see [“Connecting to the CLI using SSH” on page 20](#) or [“Connecting to the CLI using Telnet” on page 21](#).

Connecting to the CLI using SSH

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

Secure Shell (SSH) provides both secure authentication and secure communications to the CLI. Supported SSH protocol versions, ciphers, and bit strengths include SSH version 2 with AES-128, 3DES, Blowfish, and SHA-1.

Requirements

- a computer with an RJ-45 Ethernet port
- a crossover Ethernet cable
- a FortiScan network interface configured to accept SSH connections (see [“Enabling access to the CLI through the network \(SSH or Telnet or CLI Console widget\)” on page 19](#))

- an SSH client such as PuTTY

To connect to the CLI using SSH

- 1 On your management computer, start PuTTY.
- 2 In *Host Name (or IP Address)*, type the IP address of a network interface on which you have enabled SSH administrative access.
- 3 In *Port*, type 22.
- 4 From *Connection type*, select SSH.
- 5 If you are connecting to the trial license of FortiScan-VM or a LENC version of FortiScan, in the Category pane on the left, go to *Connection > SSH* to display SSH protocol-specific settings. In *Preferred SSH protocol version*, select 1. In *Encryption cipher selection policy*, select DES and click the *Up* button until it is at the top of the list. (RC2, RC4, and DES with less than 64-bit strength is supported. AES and 3DES is **not** supported in these versions.)
- 6 Click *Open*.

The SSH client connects to the FortiScan unit.

The SSH client may display a warning if this is the first time you are connecting to the FortiScan unit and its SSH key is not yet recognized by your SSH client, or if you have previously connected to the FortiScan unit but it used a different IP address or SSH key. If your management computer is directly connected to the FortiScan unit with no network hosts between them, this is normal.

- 7 Click *Yes* to verify the fingerprint and accept the FortiScan unit's SSH key. You will not be able to log in until you have accepted the key.

The CLI displays a login prompt.

- 8 Type a valid administrator account name (such as `admin`) and press Enter.
- 9 Type the password for this administrator account and press Enter.



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

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

Connecting to the CLI using Telnet

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



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

Requirements

- a computer with an RJ-45 Ethernet port
- a crossover Ethernet cable
- a FortiScan network interface configured to accept Telnet connections (see “[Enabling access to the CLI through the network \(SSH or Telnet or CLI Console widget\)](#)” on page 19)
- terminal emulation software such as PuTTY

To connect to the CLI using Telnet

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



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

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

Command syntax

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

Fortinet documentation uses the following conventions to describe valid command syntax

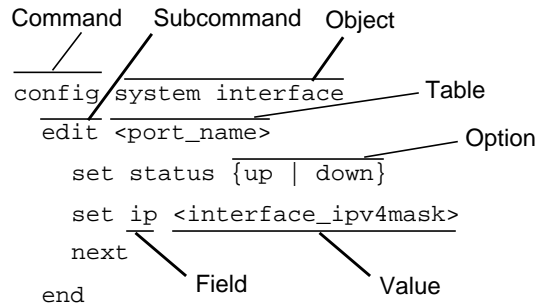
Terminology

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

```
get system admin
```

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

Figure 1: Command syntax terminology



- **command** — A word that begins the command line and indicates an action that the FortiScan appliance should perform on a part of the configuration or host on the network, such as `config` or `execute`. Together with other words, such as fields or values, that end when you press the Enter key, it forms a command line. Exceptions include multi-line command lines, which can be entered using an escape sequence. (See “Shortcuts and key commands” on page 29.)

Valid command lines must be unambiguous if abbreviated. (See “Command abbreviation” on page 29.) Optional words or other command line permutations are indicated by syntax notation. (See “Notation” on page 24.)



Note: This CLI Reference is organized alphabetically by the name of the command for top-level commands.

- **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 nested commands. (See “Indentation” on page 23.)
Not all top-level commands have sub-commands. Available sub-commands vary by their containing scope. (See “Sub-commands” on page 25.)
- **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 possibly multiple similar sets which each have a name or number, such as an administrator account, policy, or network interface. These named or numbered sets are sometimes referenced by other parts of the configuration that use them. (See “Notation” on page 24.)
- **field** — The name of a setting, such as `ip` or `hostname`. Fields in some tables must be configured with values. Failure to configure a required field will result in an invalid object configuration error message, and the FortiScan appliance will discard the invalid table.
- **value** — A number, letter, IP address, or other type of input that is usually your configuration setting held by a field. Some commands, however, require multiple input values which may not be named but are simply entered in sequential order in the same command line. Valid input types are indicated by constraint notation. (See “Notation” on page 24.)
- **option** — A kind of value that must be one or more words from a fixed set of options. (See “Notation” on page 24.)

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

For information about available sub-commands, see “Sub-commands” on page 25.

Notation

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

Table 2: Command syntax notation

Convention	Description
Square brackets []	A non-required word or series of words. For example: [verbose {1 2 3}] indicates that you may either omit or type both the <code>verbose</code> word and its accompanying option, such as: verbose 3
Curly braces { }	A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [].
Options delimited by vertical bars	Mutually exclusive options. For example: {enable disable} indicates that you must enter either <code>enable</code> or <code>disable</code> , but must not enter both.
Options delimited by spaces	Non-mutually exclusive options. For example: {http https ping snmp ssh telnet} indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: ping https ssh Note: To change the options, you must re-type the entire list. For example, to add <code>snmp</code> to the previous example, you would type: ping https snmp ssh If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.

Table 2: Command syntax notation

Angle brackets < >	<p>A word constrained by data type.</p> <p>To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_) and suffix that indicates the valid data type. For example:</p> <pre><retries_int></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"> • <xxx_name>: A name referring to another part of the configuration, such as <code>policy_A</code>. • <xxx_index>: An index number referring to another part of the configuration, such as 0 for the first static route. • <xxx_pattern>: A regular expression or word with wild cards that matches possible variations, such as <code>*@example.com</code> to match all email addresses ending in <code>@example.com</code>. • <xxx_fqdn>: A fully qualified domain name (FQDN), such as <code>mail.example.com</code>. • <xxx_email>: An email address, such as <code>admin@mail.example.com</code>. • <xxx_ipv4>: An IPv4 address, such as <code>192.168.1.99</code>. • <xxx_v4mask>: A dotted decimal IPv4 netmask, such as <code>255.255.255.0</code>. • <xxx_ipv4mask>: A dotted decimal IPv4 address and netmask separated by a space, such as <code>192.168.1.99 255.255.255.0</code>. • <xxx_ipv4/mask>: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as <code>192.168.1.99/24</code>. • <xxx_ipv4range>: A hyphen (-)-delimited inclusive range of IPv4 addresses, such as <code>192.168.1.1-192.168.1.255</code>. • <xxx_str>: A string of characters that is not 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 “Special characters” on page 29. • <xxx_int>: An integer number that is not another data type, such as 15 for the number of minutes.
---------------------------------	---

Sub-commands

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

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

```
get system admin
```

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

```
config system 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 global
  config system interface
    edit port1
```

```
        set status up
        next
    end
end
```



Note: Sub-command scope is indicated in this CLI Reference by indentation. See [“Indentation” on page 23](#).

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

- commands affecting fields (see [“Field commands” on page 28](#))
- commands affecting tables (see [“Table commands” on page 27](#))



Note: Syntax examples for each top-level command in this CLI Reference 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, such as `edit` or `next`, are available.

Table commands

Table 3: Commands for tables

Sub-command	Description
delete <table_name>	Remove a table from the current object. For example, in <code>config system admin</code> , you could delete an administrator account named <code>newadmin</code> by typing <code>delete newadmin</code> and pressing Enter. This deletes <code>newadmin</code> and all its fields, such as <code>newadmin</code> 's first-name and email-address. <code>delete</code> is only available within objects containing tables.
edit <table_name>	Create or edit a table in the current object. <code>edit</code> is an interactive sub-command: further sub-commands are available from within <code>edit</code> . <code>edit</code> changes the prompt to reflect the table you are currently editing. <code>edit</code> is only available within objects containing tables.
end	Save the changes to the current object and exit the <code>config</code> command. This returns you to the top-level command prompt.
get	List the configuration of the current object or table. <ul style="list-style-type: none"> In objects, <code>get</code> lists the table names (if present), or fields and their values. In a table, <code>get</code> lists the fields and their values. For more information on <code>get</code> commands, see “get” on page 93 .
purge	Remove all tables in the current object. <code>purge</code> is only available for objects containing tables. Caution: Back up the FortiScan appliance before performing a <code>purge</code> . <code>purge</code> cannot be undone. To restore purged tables, the configuration must be restored from a backup. For details, see “execute backup config” on page 64 . Caution: Do not purge <code>system interface</code> or <code>system admin</code> tables. <code>purge</code> does not provide default tables. This can result in being unable to connect or log in, requiring the FortiScan appliance to be formatted and restored.
rename <table_name> to <table_name>	Rename a table. For example, in <code>config system admin</code> , you could rename <code>admin3</code> to <code>fwadmin</code> by typing <code>rename admin3 to fwadmin</code> . <code>rename</code> is only available within objects containing tables.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands. For more information on <code>show</code> commands, see “show” on page 139 .

Example of table commands

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

```
edit 2
```

The CLI changes the command prompt to show that you are now within the 2 table:

```
(2)#
```

Field commands

Table 4: Commands for fields

Sub-command	Description
abort	Exit both the <code>edit</code> and/or <code>config</code> commands without saving the fields.
end	Save the changes made to the current table or object fields, and exit the <code>config</code> command. (To exit without saving, use <code>abort</code> instead.)
get	List the configuration of the current object or table. <ul style="list-style-type: none"> In objects, <code>get</code> lists the table names (if present), or fields and their values. In a table, <code>get</code> lists the fields and their values.
next	Save the changes you have made in the current table's fields, and exit the <code>edit</code> command to the object prompt. (To save and exit to the previous level of command prompt, use <code>end</code> instead.) <code>next</code> is useful when you want to create or edit several tables in the same object, without leaving and re-entering the <code>config</code> command each time. <code>next</code> is only available from a table prompt; it is not available from an object prompt.
set <field> <value>	Set a field's value. For example, in <code>config system route</code> , after typing <code>edit 1</code> , you could type <code>set device port1</code> to change the outgoing network interface of the route whose index number is 1 to <code>port1</code> . Note: When using <code>set</code> to change a field containing a space-delimited list, type the whole new list. For example, <code>set <field> <new-value></code> will replace the list with the <code><new-value></code> rather than appending <code><new-value></code> to the list.
show	Display changes to the default configuration. Changes are listed in the form of configuration commands.
unset <field>	Reset the table or object's fields to default values. For example, in <code>config system admin</code> , after typing <code>edit admin</code> , typing <code>unset password</code> resets the password of the admin administrator account to the default (in this case, no password).

Example of field commands

From within the route table whose index number is 2, you might enter:

```
set device port1
```

to assign the value `port1` to the `device` field. You might then enter the `next` command to save the changes and edit the next static route's table.

Tips and tricks

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

This section includes:

- [Help](#)
- [Shortcuts and key commands](#)
- [Command abbreviation](#)
- [Special characters](#)
- [Language support](#)
- [Screen paging](#)
- [Baud rate](#)

- [Editing the configuration file on an external host](#)

Help

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

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Type a word or part of a word, then press the question mark (?) key to display a list of valid word completions or subsequent words, and to display a description of each.

Shortcuts and key commands

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

Command abbreviation

You can abbreviate words in the command line to their smallest number of non-ambiguous characters.

For example, the command `get system status` could be abbreviated to `g sy st.`

Special characters

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

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

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 ñ, é, symbols, and ideographs are sometimes acceptable input. Support varies by the nature of the item being configured. CLI commands, objects, field names, and options must use their exact ASCII characters, but some items with arbitrary names or values may be input using your language of choice.

For example, the host name must not contain special characters, and so the web UI and CLI will not accept most symbols and other non-ASCII encoded characters as input when configuring the host name. This means that languages other than English often are not supported. However, some configuration items, such as names and comments, may be able to use the language of your choice.

To use other languages in those cases, you must use the correct encoding.

It is simplest to use only US-ASCII characters when configuring the FortiScan appliance using the web UI or CLI. 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 UI
- 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 using non-ASCII characters, verify that all systems interacting with the FortiScan appliance also support the same encodings. You should also use the same encoding throughout the configuration if possible in order to avoid needing to switch the language settings of the web UI and your web browser or Telnet/SSH client while you work.

Similarly to input, your web browser or CLI client should usually interpret display output as encoded using UTF-8. If it does not, your configured items may not display correctly in the web UI or CLI.

Screen paging

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

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

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

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

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

For more information, see [“system console” on page 35](#).

Baud rate

You can change the default baud rate of the local console connection. For more information, see [“system console” on page 35](#).

Editing the configuration file on an external host

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

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

To edit the configuration on your computer

- 1 Use [execute backup config](#) to download the configuration file to a TFTP server, such as your management computer.
- 2 Edit the configuration file using a plain text editor that supports Unix-style line endings.



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

- 3 Use `execute restore config` to upload the modified configuration file back to the FortiScan appliance.

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

config global

The sub-commands within `config global` configure your FortiScan appliance's system-wide settings. Sub-commands use the following syntax:

```
config global
  config ...
  diagnose ...
  execute ...
end
```

This chapter describes the following sub-commands within `config global`:

<code>config gui console</code>	<code>config system global</code>	<code>config system route</code>
<code>config system console</code>	<code>config system interface</code>	<code>config system snmp</code>
<code>config system dns</code>	<code>config system ntp</code>	
	<code>config system raid</code>	

gui console

Use this command to configure the web UI's *CLI Console* widget.

Syntax

```
config global
  config gui console
    set preferences <filedata_str>
  end
end
```

Variable	Description	Default
preferences <filedata_str>	Upload the Base64-encoded file that contains preferences for the web UI's <i>CLI Console</i> widget.	No default.

Related topics

- [config system console](#)
- [config system global](#)

system console

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

Syntax

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

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

Example

This example sets the baud rate to 9600.

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

Related topics

- [config system global](#)

system dns

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

Syntax

```
config global
  config system dns
    set primary <dns_ipv4>
    set secondary <dns_ipv4>
  end
end
```

Variable	Description	Default
primary <dns_ipv4>	Enter the primary DNS server IP address.	0.0.0.0
secondary <dns_ipv4>	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 global
  config system dns
    set primary 172.16.35.133
    set secondary 172.16.25.132
  end
end
```

Related topics

- [config system fortiguard](#)
- [config system mail](#)
- [config system ntp](#)

system fortiguard

Use this command to configure connections to the FortiGuard Distribution Network (FDN), including vulnerability management settings, such as proxy server and scheduling of updates of FortiGuard Vulnerability Management Service (VCM) packages.

Syntax

```
config global
  config system fortiguard
    set fds-override-addr <fds_ipv4>
    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_int>
    set vm-minute <minutes_int>
    set vm-proxy {enable | disable}
    set vm-proxy-ip <proxy_ipv4>
    set vm-proxy-passwd <password_str>
    set vm-proxy-port <port_int>
    set vm-proxy-user <user_str>
    set vm-schedule {enable | disable}
  end
end
```

Variable	Description	Default
fds-override-addr <fds_ipv4>	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_int>	Enter the hour of when to update the vulnerability management services. The hours are from 0-23.	1
vm-minute <minutes_int>	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 <proxy_ipv4>	Enter the IP address of the SSL proxy server.	No default
vm-proxy-passwd <password_str>	Enter the user name's password for logging in to the SSL proxy server.	No default
vm-proxy-port <port_int>	Enter the port of the SSL proxy server.	8080

Variable	Description	Default
vm-proxy-user <user_str>	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 configures a daily schedule for FortiGuard update requests and disables the automatically generated vulnerability report.

```
config global
  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
end
```

Related topics

- [config system dns](#)

system global

Use this command to configure the host name, time zone, web UI language, and idle timeout.

Syntax

```
config global
  config system global
    set admintimeout <timeout_int>
    set hostname <host_str>
    set language {english}
    set timezone <timezone_int>
  end
end
```

Variable	Description	Default
admintimeout <timeout_int>	Type the maximum amount of time (in minutes) that an administrative session can be inactive (e.g., there are no new page requests for the web UI). If the session is idle longer than this value, the FortiScan appliance automatically logs out the administrator. To continue using the appliance, the administrator must log in again. The maximum value is 480 minutes (8 hours). To improve security, keep the idle timeout at its default value. Note: Sessions will not time out when viewing real-time logs.	5
hostname <host_str>	Type the host name of this FortiScan appliance.	Varies by model. Example: FortiScan-3000C
language {english}	Type the display language of the web UI. Currently, only English is supported.	english
timezone <timezone_int>	Type the number corresponding to the time zone where the FortiScan appliance is installed. To display a list of time zones and their numbers, enter <code>set timezone ?</code>	00

Example

This example shows how to change the host name.

```
config global
  config system global
    set hostname corporate_scanner
  end
end
```

Related topics

- [config gui console](#)
- [config system interface](#)
- [config system ntp](#)
- [execute set-date](#)
- [execute set-time](#)
- [diagnose gui console](#)

system interface

Use this command to configure the network interfaces of the FortiScan appliance.



Caution: On FortiScan-VM, after 5 changes of the IP address that is bound to the license, administrators will be locked out of the web UI until you request and upload a new license.

Syntax

```
config global
  config system interface
    edit <interface_name>
      set allowaccess {http https ping ssh telnet}
      set ip <interface_ipv4> <interface_ipv4mask>
      set lockout {enable | disable}
      set mtu-override {enable | disable}
      set mtu <bytes_int>
      set speed {1000baseT_Full | 100baseT_Full | 100baseT_Half |
        10baseT_Full | 10baseT_Half | Speed_unknown | auto}
      set status {down | up}
    end
  end
end
```

Variable	Description	Default
<interface_name>	Type the name of the network interface, such as port1.	No default.
allowaccess {http https ping ssh telnet}	Select the types of management access permitted on this interface. Separate each access type with a space, such as ping https ssh. If you want to add or remove an option from the list, retype the entire space-delimited list.	Varies by interface.
ip <interface_ipv4> <interface_ipv4mask>	Type the IP address and subnet mask of the interface. Note: The IP address cannot be on the same subnet as any other interface.	Varies by interface.
lockout {enable disable}	Enable to temporarily prevent further login attempts if an administrator fails to log in after three attempts. This option can be used to deter brute force login attacks.	disable
mtu-override {enable disable}	Enable to override the maximum transmission unit (MTU). Also configure mtu <bytes_int> .	disable
mtu <bytes_int>	Enter the maximum packet or Ethernet frame size in bytes. If network devices between the FortiMail unit and its traffic destinations require smaller or larger units of traffic, packets may require additional processing at each node in the network to fragment or defragment the units, resulting in reduced network performance. Adjusting the MTU to match your network can improve network performance. The valid range is from 576 to 1500 bytes. This setting is applicable only if mtu-override is enable.	1500

Variable	Description	Default
<pre>speed {1000baseT_Full 100baseT_Full 100baseT_Half 10baseT_Full 10baseT_Half Speed_unknown auto}</pre>	<p>Select the speed of the physical network link:</p> <ul style="list-style-type: none"> • auto: Use auto-negotiation to determine the link speed. • Speed_unknown: Use if the speed and auto-negotiation support is not known. • 10baseT_Full: 10 Mbps, full duplex • 10baseT_Half: 10 Mbps, half duplex • 100baseT_Full: 100 Mbps, full duplex • 100baseT_Half: 100 Mbps, half duplex • 1000baseT_Full: 1000 Mbps, full duplex <p>Speed options may vary for different models and ports. To display a list of speeds available for your model and interface, type <code>set speed ?</code>.</p> <p>Tip: Configure the speed only if the port is linked to another device that does not support auto-negotiation.</p>	auto
<pre>status {down up}</pre>	<p>Select <code>up</code> to bring up the network interface so that it is permitted to receive or transmit traffic.</p>	up

Example

This example enables `port1` and sets its IP address to `192.168.1.10` and its netmask to `255.255.255.0`, and allows ICMP ping, HTTPS, and SSH management access connections to that interface.

```
config global
  config system interface
    edit port1
      set status up
      set allowaccess ping https ssh
      set ip 192.168.1.10 255.255.255.0
    end
  end
```

Related topics

- [config system global](#)
- [config system route](#)
- [config system snmp](#)
- [diagnose netlink](#)
- [diagnose sniffer packet](#)

system mail

Use this command to configure SMTP settings to enable the FortiScan appliance to send alert messages via email.



Note: This command applies only for network vulnerability scan alert messages.

Syntax

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

Variable	Description	Default
<server_name>	Type the IP address or fully qualified domain name (FQDN) of the SMTP server. This will also be used as the name for this SMTP settings entry.	No default.
auth {enable disable}	Enable if the SMTP server requires SMTP authentication.	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_email>	Enter the 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 adds settings enabling the appliance to send alerts using an SMTP mail server.

```
config global
  config system mail
    edit smtp.example.com
      set auth enable
      set user FortiScan@smtp.example.com
      set passwd s3cr3t
    end
  end
```

Related topics

- [config system dns](#)
- [config report output](#)
- [diagnose alertmail error-msg](#)

system ntp

Use this command to configure synchronization of the FortiScan unit's system time with Network Time Protocol (NTP) servers.

Syntax

```
config global
  config system ntp
    set ntpsync {enable | disable}
    set syncinterval <interval_int>
  config ntpserver
    edit <ntp_index>
      set server {<server_ipv4> | <server_fqdn>}
    end
  end
end
```

Variable	Description	Default
ntpsync {enable disable}	Enable synchronization of the FortiScan appliance's system time with an NTP server or pool.	disable
syncinterval <interval_int>	Type the interval in minutes between each query that the FortiScan appliance sends to the NTP server or pool. Valid values range from 1 to 1440 minutes. This setting is only available when ntpsync is enable.	0
<ntp_index>	Type the index number that identifies the table entry.	No default.
server {<server_ipv4> <server_fqdn>}	Type the IP address or fully qualified domain name (FQDN) of a Network Time Protocol (NTP) server or pool to query in order to synchronize the FortiScan appliance's clock. For more information about NTP and to find the IP address of an NTP server that you can use, see http://www.ntp.org/ .	No default.

Example

This example enables synchronization with the NTP server whose domain name is pool.ntp.org. The appliance synchronizes every 100 minutes.

```
config global
  config system ntp
    set ntpsync enable
    set syncinterval 100
  config ntpserver
    edit server1
      set ip pool.ntp.org
    end
  end
end
```

Related topics

- [config system dns](#)
- [execute set-date](#)
- [execute set-time](#)
- [diagnose ntpd](#)

system raid

Use the this command to configure RAID levels.

Syntax

```
config global
  config system raid
    set level {raid10 | raid0 | raid1 | raid5}
  end
end
```

Variable	Description	Default
level {raid10 raid0 raid1 raid5}	Enter the level of RAID you want for your FortiScan appliance. Note: Valid RAID levels depend on the number of hard drives in your FortiScan model.	No default.

Example

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

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

Related topics

- [get system status](#)
- [diagnose raid](#)

system route

Use these commands to configure static routes.

Syntax

```
config global
  config system route
    edit <index_int>
      set device {port1 | port2 | port3 | port4}
      set dst <destination_ipv4> <destination_ipv4mask>
      set gateway <gateway_ipv4>
    end
  end
end
```

Variable	Description	Default
<index_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_ipv4> <destination_ipv4mask>	Enter the destination IP address and network mask for this route. To create a default route, type 0.0.0.0 0.0.0.0.	0.0.0.0 0.0.0.0
gateway <gateway_ipv4>	Enter the IP address of the next-hop router to which traffic is forwarded.	0.0.0.0

Example

This example adds a static route that has the sequence number 2.

```
config global
  config system route
    edit 2
      set device port1
      set dst 192.168.22.0 255.255.255.0
      set gateway 192.168.1.2
    end
  end
end
```

Related topics

- [config system interface](#)
- [diagnose netlink](#)

system snmp

Use this command to configure which SNMP managers can query the appliance and receive traps for alert messages.

Syntax

```
config global
  config system snmp community
    edit events {cpu-high | mem-low | log-full | system_event | raid}
    set events {cpu-high | mem-low | log-full | system_event | raid}
    set query-v1-port <port_int>
    set query-v1-status {enable | disable}
    set query-v2c-port <port_int>
    set query-v2c-status {enable | disable}
    set status {enable | disable}
    set trap-v1-lport <port_int>
    set trap-v1-rport <port_number>
    set trap-v1-status {enable | disable}
    set trap-v2c-lport <port_int>
    set trap-v2c-rport <port_int>
    set trap-v2c-status {enable | disable}
  end
end
```

Variable	Description	Default
<snmp_name>	Type the IP address or fully qualified domain name (FQDN) of the SNMP manager.	No 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_int>	Enter the SNMP query port number.	161
query-v1-status {enable disable}	Enable the SNMP v1 query.	enable
query-v2c-port <port_int>	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_int>	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_int>	Enter the SNMP v2c trap local port number.	162

Variable	Description	Default
trap-v2c-rport <port_int>	Enter the SNMP v2c trap remote port number.	162
trap-v2c-status {enable disable}	Disable to not configure the SNMP v2c trap.	enable

```

config global
  config system snmp sysinfo
    set agent {enable | disable}
    set contact-info <contact_str>
    set description <description_str>
    set location <location_str>
  end
end

```

Variable	Description	Default
agent {enable disable}	Enable the SNMP agent.	disable
contact-info <contact_str>	Enter an administrative contact for the SNMP server.	No default.
description <description_str>	Enter a description for the server.	No default.
location <location_str>	Enter the location of the server.	No default.

```

config global
  config system snmp traps {cpu | memory | disk}
    set frequency <seconds_int>
    set period <seconds_int>
    set threshold <triggers_int>
    set trigger <percentage_int>
  end
end

```

Variable	Description	Default
traps {cpu memory disk}	Enter to configure traps for CPU, Memory or Disk.	No default
frequency <seconds_int>	Enter a time period, in seconds, for the frequency of the traps that occur.	No default
period <seconds_int>	Enter a time period, in seconds.	No default
threshold <triggers_int>	Enter a number for the number of triggers that occur before sending a trap.	No default
trigger <percentage_int>	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 global
  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
end
```

Related topics

- [config system interface](#)

config adom

The sub-commands within `config adom` configure settings for a specific administrative domain (ADOM) on your FortiScan appliance. Sub-commands use the following syntax:

```
config adom
  edit <adom_name>
    config ...
    execute vm ...
  end
end
```

This chapter describes the following sub-commands within `config adom`:

- `config report output`
- `config system mail`
- `config vm map-config`
- `config vm scan-profile`
- `config vm schedule`
- `config vm sensor`

report output

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

Syntax

```
config report output
  edit <output_name>
    set description
    set email {enable | disable}
    set email-subject <subject_str>
    set email-body <body_str>
    set email-attachment-name <attachment_str>
    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 | sftp | scp}
    set upload-server <class_ip>
    set upload-user <user_str>
    set upload-pass <password_str>
    set upload-dir <directory_str>
    set upload-delete {enable | disable}
    set upload-compress {enable | disable}
  end
end
```

Variable	Description	Default
<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 <subject_str>	Enter a subject line for the email.	No default.
email-body <body_str>	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_str>	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

Variable	Description	Default
upload-server-type {ftp sftp scp}	Enter the protocol to use when configuring the uploading server.	No default.
upload-server <class_ip>	Enable or disable to configure a server.	No default.
upload-user <user_str>	Enter the user name for accessing the server.	No default.
upload-pass <password_str>	Enter the password for accessing the server.	No default.
upload-dir <directory_str>	Enter the directory path where the FortiScan appliance saves the generated report on the server.	No default.
upload-delete {enable disable}	Enable or disable the option to delete the completed report from the FortiScan appliance's hard disk once it has been completely uploaded to the remote server.	disable
upload-compress {enable disable}	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

```

Related topics

- [config system mail](#)
- [config vm map-config](#)
- [config vm scan-profile](#)
- [config vm schedule](#)
- [config vm sensor](#)
- [execute vm](#)

system mail

Use this command to configure SMTP settings to enable the FortiScan appliance to send alert messages via email.



Note: This command applies only for network vulnerability scan alert messages.

Syntax

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

Variable	Description	Default
<server_name>	Type the IP address or fully qualified domain name (FQDN) of the SMTP server. This will also be used as the name for this SMTP settings entry.	No default.
auth {enable disable}	Enable if the SMTP server requires SMTP authentication.	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_email>	Enter the 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 adds settings enabling the appliance to send alerts using an SMTP mail server.

```
config global
  config system mail
    edit smtp.example.com
      set auth enable
      set user FortiScan@smtp.example.com
      set passwd s3cr3t
    end
  end
end
```

Related topics

- [config system dns](#)
- [config report output](#)
- [diagnose alertmail error-msg](#)

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 <asset_ipv4> [<ipv4> <ipv4>...]
    set asset-group <group_name>
    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 <asset_ipv4> [<ipv4> <ipv4>...]	Enter one or more IP addresses of approved hosts. Separate each IP address with a space.	No default.
asset-group <group_name>	Enter the name of 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 appliance scans.	No default
live-host-sweep {enable disable}	Enable to have the FortiScan appliance 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"> <code>daily</code> has the FortiScan appliance 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. <code>weekly</code> has the FortiScan appliance 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. <code>monthly</code> has the FortiScan 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. 	daily
schedule {run-now run-later}	Specify whether the schedule will run once or at regular intervals. <ul style="list-style-type: none"> <code>run-now</code> will have the FortiScan appliance run the specified map configuration immediately, and only once. <code>run-later</code> will have the FortiScan appliance run the map configuration at regular intervals, as specified with the <code>recurrence</code> command. 	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
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
```

Related topics

- [config vm scan-profile](#)
- [config vm schedule](#)
- [config vm sensor](#)
- [execute vm](#)

vm scan-profile

Scan profiles are used to define exactly what means a network vulnerability scan uses 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 appliance 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 appliance 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"> • <code>full</code> scans all TCP ports. This is the most thorough scan, but it also takes the longest. • <code>standard</code> scans about 1800 of the most commonly used TCP ports. • <code>light</code> scans about 160 of the most commonly used TCP ports. • <code>none</code> disables the TCP port scan. 	none
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"> • <code>full</code> scans all UDP ports. This is the most thorough scan, but it also takes the longest. • <code>standard</code> scans about 180 of the most commonly used UDP ports. • <code>light</code> scans about 30 of the most commonly used UDP ports. • <code>none</code> disables the UDP port scan. 	none

Example

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

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

Related topics

- [config report output](#)
- [config vm map-config](#)
- [config vm schedule](#)
- [config vm sensor](#)
- [execute vm](#)

vm schedule

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

Syntax

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

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

Variables	Description	Default
recurrence {daily weekly monthly}	Enter how often a scheduled scan is run. <ul style="list-style-type: none"> daily has the FortiScan appliance run the scan once a day. Use the hour and minute commands to specify when during the day the scan is run. weekly has the FortiScan appliance run the scan once a week. Use the day-of-week, hour, and minute commands to specify when during the week the scan is run. monthly has the FortiScan appliance run the scan once a month. Use the day-of-month, hour, and minute commands to specify when during the month the scan is run. 	daily
scan-profile <profile_str>	Enter the name of the scan profile to use.	No default
schedule {run-now run-later}	Specify whether the schedule will run once or at regular intervals. <ul style="list-style-type: none"> run-now will have the FortiScan appliance run the schedule immediately, and only once. run-later will have the FortiScan appliance run the schedule at regular intervals, as specified with the recurrence command. 	run-now

Example

This example details the commands required to create a vulnerability 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
```

Related topics

- [config report output](#)
- [config vm map-config](#)
- [config vm scan-profile](#)
- [config vm sensor](#)
- [execute vm](#)

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 <date_str>
        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 <date_str>
        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 <fid_str>
      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 appliance authenticate with the hosts to be scanned. Enter the vulnerabilities to include by the authentication they require. Enter the required options, or enter none to indicate no authentication.	No default.
bug {existent ignore nonexistent}	Include vulnerabilities depending on whether they've been assigned a Bug Traq ID. <ul style="list-style-type: none"> existent - restrict the included vulnerabilities to only those with a Bug Traq ID. nonexistent - restrict the included vulnerabilities to only those without a Bug Traq ID. ignore - do not restrict the included vulnerabilities based on whether they have been assigned a Bug Traq ID. 	ignore

Variables	Description	Default
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"> <code>existent</code> - restrict the included vulnerabilities to only those with a CVE ID. <code>nonexistent</code> - restrict the included vulnerabilities to only those without a CVE ID. <code>ignore</code> - do not restrict the included vulnerabilities based on whether they have been assigned a CVE ID. 	ignore
end-date <date_str>	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"> <code>yes</code> - restrict the included vulnerabilities to only those that have been detected in previous scans using this sensor. <code>no</code> - restrict the included vulnerabilities to only those that have not been detected in previous scans using this sensor. <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. 	ignore
fid <fid_str>	Enter the Fortinet Vulnerability ID. Separate multiple FID numbers with commas.	No default.
ips {existent ignore nonexistent}	Include vulnerabilities depending on whether they are also FortiGuard IPS signatures. <ul style="list-style-type: none"> <code>existent</code> - Restrict the included vulnerabilities to only those that are FortiGuard IPS signatures. <code>nonexistent</code> - Restrict the included vulnerabilities to only those that are not FortiGuard IPS signatures. <code>ignore</code> - Do not restrict the included vulnerabilities based on whether they are FortiGuard IPS signatures. 	ignore
patch {existent ignore nonexistent}	Include vulnerabilities depending on whether a patch exists to fix them. <ul style="list-style-type: none"> <code>existent</code> - restrict the included vulnerabilities to only those with a patch. <code>nonexistent</code> - restrict the included vulnerabilities to only those without a patch. <code>ignore</code> - do not restrict the included vulnerabilities based on whether they have a patch. 	ignore
severity {information low medium high critical}	All vulnerabilities are assigned a relative severity level. Enter the severity levels to include in the filter. Enter all five severity levels to effectively disable severity as a means of limiting the vulnerabilities included in the filter.	No default.

Variables	Description	Default
start-date <date_str>	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"> • <i>existent</i> - restrict the included vulnerabilities to only those with a link. • <i>nonexistent</i> - restrict the included vulnerabilities to only those without a link. • <i>ignore</i> - do not restrict the included vulnerabilities based on whether they have a vendor reference link. 	ignore

Example

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

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

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

Related topics

- [config report output](#)
- [config vm map-config](#)
- [config vm scan-profile](#)
- [config vm schedule](#)
- [execute vm](#)

execute

The `execute` commands perform immediate operations on the FortiScan appliance. These commands can:

- back up and restore the system configuration
- reset the appliance to default settings
- set the system date and time
- diagnose network problems by using ping
- update FortiGuard Vulnerability Management Service engines and packages



Note: Most `execute` commands are global in scope, and are only available from within `config global`. Exceptions include `execute vm`, which is available from within `config adm`.

This chapter contains the following sections:

execute backup config	execute ping-options	execute restore vm
execute backup config-secure	execute reboot	execute set-date
execute disconnect	execute reload	execute set-time
execute em_dbbackup	execute remove	execute shutdown
execute em_dbrestore	execute reset_password	execute traceroute
execute factoryreset	execute restore config	execute upload-benchmark
execute ping	execute restore config-secure	execute vm
	execute restore image	

backup config

Use this command to upload a plain text backup of the configuration file to a server.



Tip: Alternatively, you can upload an encrypted backup file. See “execute backup config-secure” on page 66.



Note: For a complete backup, you must back up **both** the configuration file and the database. For the command to back up the configuration file, see “execute em_dbbackup” on page 69.

Syntax

```
config global
  execute backup config {ftp | sftp | scp | tftp} {<server_ipv4> |
    <server_fqdn>} <argument1_str> <argument2_str> <argument3_str>
    [<argument4_str>]
```

Variable	Description	Default
{ftp sftp scp tftp}	Choose which protocol to use to connect to the server. With SSH servers, use SCP.	No default.
{<server_ipv4> <server_fqdn>}	Type the IP address or domain name of the server. Note: Domain names are currently not valid input with this command if you choose the FTP protocol.	No default.
<argument1_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the user name that the FortiScan appliance will use to authenticate when connecting to the server. For TFTP, type the directory path on the server where the backup will be uploaded. 	No default.
<argument2_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the password, if any. If there is no password, type a hyphen (-). For TFTP, type the file name of the backup. 	No default.
<argument3_str>	Type the directory path on the server where the backup will be uploaded. This argument is not applicable when using the command with TFTP.	No default.
[<argument4_str>]	Optional. If you do not want to use the default file name, type a file name for the backup. This argument is not applicable when using the command with TFTP.	No default.

Example

This example uploads a FortiScan-3000C configuration file backup to a file named `fsc3000c.cfg` in the directory named `fortiscan-configs` in the home directory of the user account named `fortiscan` on an SSH server at IP address `192.168.1.23`.

```
FortiScan-3000C # config global
global # execute backup config scp 192.168.1.23 fortiscan P@ssword1
fortiscan-configs fortiscan-3000c.cfg
```

A prompt appears, asking you for the password to use when encrypting the backup file:

Password for the secured file:

Type a password for the file, then press Enter. A message appears:

```
Please wait...
Connect to scp server 192.168.1.23 ...
```

Time required to upload the file varies by the size of the file and the speed of the network connection. If the backup succeeds, a message similar to the following appears:

```
Successfully sent config file to scp server 192.168.1.23 under fortiscan-  
configs.
```

To restore config file, execute the following command:

```
execute restore config scp 192.168.1.23 <user_name> <password> fortiscan-  
configs fortiscan-3000c.cfg
```

If the appliance **cannot** connect to the server, an error message similar to the following appears:

```
connect: No route to host
```

```
Sending config file to ftp server 192.168.1.23 failed.  
Command fail. Return code 3
```

Related topics

- [execute backup config-secure](#)
- [execute em_dbbackup](#)
- [execute factoryreset](#)
- [execute reload](#)
- [execute restore config](#)
- [diagnose cmdb](#)

backup config-secure

Use this command to upload an encrypted backup of the configuration file to a server.



Tip: Alternatively, you can upload a plain text backup file. See “execute backup config” on page 64.



Note: For a complete backup, you must back up **both** the configuration file and the database. For the command to back up the configuration file, see “execute em_dbbackup” on page 69.

Syntax

```
config global
  execute backup config-secure {ftp | sftp | scp | tftp} {<server_ipv4> |
    <server_fqdn>} <argument1_str> <argument2_str> <argument3_str>
    <argument4_str> <argument5_str>
```

Variable	Description	Default
{ftp sftp scp tftp}	Choose which protocol to use to connect to the server. With SSH servers, use SCP.	No default.
{<server_ipv4> <server_fqdn>}	Type the IP address or domain name of the server. Note: Domain names are currently not valid input with this command if you choose the FTP protocol.	No default.
<argument1_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the user name that the FortiScan appliance will use to authenticate when connecting to the server. For TFTP, type the directory path on the server where the backup will be uploaded. 	No default.
<argument2_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the password, if any. If there is no password, type a hyphen (-). For TFTP, type the file name of the backup. 	No default.
<argument3_str>	Type the directory path on the server where the backup will be uploaded. This argument is not applicable when using the command with TFTP.	No default.
<argument4_str>	Type a file name for the backup.	No default.
<argument5_str>	Type the password that will be used to encrypt the backup file. Caution: Do not lose this password. You will need to enter this same password when restoring the backup file in order for the appliance to successfully decrypt the file. If you cannot remember the password, the backup cannot be used.	No default.

Example

This example uploads a FortiScan-3000C configuration file backup to a file named `fsc3000c.cfg` in the directory named `fortiscan-configs` in the home directory of the user account named `fortiscan` on an SSH server at IP address `192.168.1.23`. The backup file is encrypted using the password `my-password`.

```
FortiScan-3000C # config global
global # execute backup config-secure scp 192.168.1.23 fortiscan P@ssword1
fortiscan-configs fortiscan-3000c.cfg my-password
```

A prompt appears, asking you for the password to use when encrypting the backup file:

Password for the secured file:

Type a password for the file, then press Enter. A message appears:

```
Please wait...
```

Time required to upload the file varies by the size of the file and the speed of the network connection. If the backup succeeds, a message similar to the following appears:

```
Successfully sent config file to scp server 192.168.1.23 under fortiscan-  
configs.
```

To restore config file, execute the following command:

```
execute restore config-secure scp 192.168.1.23 <user_name> <password>  
fortiscan-configs fortiscan-3000c.cfg <password>
```

If the appliance **cannot** connect to the server, an error message similar to the following appears:

```
connect: No route to host
```

```
Sending config file to ftp server 192.168.1.23 failed.  
Command fail. Return code 3
```

Related topics

- [execute backup config](#)
- [execute em_dbbackup](#)
- [execute factoryreset](#)
- [execute reload](#)
- [execute restore config-secure](#)
- [diagnose cmdb](#)

disconnect

Use this command to disconnect an administrator from the web UI or CLI of the FortiScan appliance by terminating their session, effectively logging them out of the system.

You can also use this command to list all current administrative sessions, including their associated administrator account, method of access, and associated IP address.

Syntax

```
config global
  execute disconnect <session_index>
```

Variable	Description	Default
disconnect <session_index>	Enter the session ID of an administrative access session. To view a list of all current administrative sessions, enter <code>execute disconnect ?</code>	No default.

Example

This example lists all administrative sessions.

```
config global
  execute disconnect ?
```

Output:

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

In the third entry, the column `Login from` contains `jsconsole`. This indicates access through the web UI's *CLI Console* widget. The source IP address of this session is the same as its corresponding web UI session.

Example

This example terminates the session whose index number is 1. (Assuming the output from the previous example, this would terminate the web UI session.) For that administrator to continue, they must log in again and start a new session.

```
config global
  execute disconnect 1
```

em_dbbackup

Use this command to upload a backup of the FortiScan appliance's database to a server.



Note: For a complete backup, you must back up **both** the configuration file and the database. For the command to back up the configuration file, see either “execute backup config” on page 64 or “execute backup config-secure” on page 66.

Syntax

```
config global
  execute em_dbbackup {ftp | scp | sftp | tftp} {<server_ipv4> |
    <server_fqdn>} <argument1_str> <argument2_str> <argument3_str>
    [<argument4_str>]
```

Variable	Description	Default
{ftp scp sftp tftp}	Choose which protocol to use to connect to the server. With SSH servers, use SCP.	No default.
{<server_ipv4> <server_fqdn>}	Type the IP address or domain name of the server. Note: Domain names are currently not valid input with this command if you choose the FTP protocol.	No default.
<argument1_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the user name that the FortiScan appliance will use to authenticate when connecting to the server. For TFTP, type the directory path on the server where the backup will be uploaded. 	No default.
<argument2_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the password, if any, or, if there is no password, type a hyphen (-). For TFTP, type the file name of the backup. 	No default.
<argument3_str>	Type the directory path on the server where the backup will be uploaded. This argument is not applicable when using the command with TFTP.	No default.
[<argument4_str>]	Optional. If you do not want to use the default file name, type a file name for the backup. This argument is not applicable when using the command with TFTP.	No default.

Example

This example backs up a FortiScan-3000C appliance's database to a file named FSC3000CDB on an FTP server at IP address 172.16.1.1. The appliance authenticates using an account named fortiscan with no password.

```
config global
  execute em_dbbackup ftp 172.16.1.1 fortiscan - ./ 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 172.16.1.1 ...
```

```
Successfully uploaded the backup file to ftp server 172.16.1.1.  
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** continue by entering `n`, the appliance's application server will not start up and you will be unable to use the web UI until you use the CLI to reboot the appliance.

Related topics

- [execute backup config](#)
- [execute backup config-secure](#)
- [execute em_dbrestore](#)
- [execute factoryreset](#)
- [execute restore config](#)
- [execute restore config-secure](#)

em_dbrestore

Use this command to restore the database of the FortiScan appliance from a backup stored on a server.



Note: For a complete restoration, you must restore **both** the configuration file and the database. For the command to restore the configuration file, see either “execute restore config” on page 81 or “execute restore config-secure” on page 82.

Syntax

```
config global
  execute em_dbrestore {ftp | sftp | scp | tftp} {<server_ipv4> |
    <server_fqdn>} <arg1_str> <arg2_str> <arg3_str> <arg4_str>
```

Variable	Description	Default
{ftp sftp scp tftp}	Select whether to restore the database from a file on a FTP, SFTP, SCP, or TFTP server.	No default.
{<server_ipv4> <server_fqdn>}	Type either the IP address or (only if not using FTP) the fully qualified domain name (FQDN) of a server where the appliance's database backup file is stored. Note: Domain names are not supported when connecting to an FTP server.	No default.
<arg1_str>	For FTP, SFTP, or SCP, enter the user name of an account that the appliance can use to log on to the server. For TFTP, enter a directory or file name.	No default.
<arg2_str>	For FTP, SFTP, or SCP, enter a password or, if there is no password, enter a hyphen (-). For TFTP, enter the file name or press Enter.	No default.
<arg3_str>	For FTP, SFTP, or SCP, enter a directory path, such as ./ / For TFTP, press Enter.	No default.
<arg4_str>	For FTP, SFTP, or SCP, type a file name and press Enter.	No default.

Example

This example restores a FortiScan-3000C database from a file named FSC3000CDB located on the FTP server at IP address 172.1.1.4, where the FortiScan appliance logs in using an account named user1 with no password.

```
config global
  execute em_dbrestore ftp 172.1.1.4 user1 - ./ 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 172.1.1.4 ...
Successfully downloaded the file from ftp server 172.1.1.4.
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 enter `n`, the appliance's application server will remain unavailable (and you will be unable to connect to the web UI) until you reboot the appliance.

Related topics

- [execute em_dbbackup](#)
- [execute factoryreset](#)
- [execute restore config](#)
- [execute restore config-secure](#)

factoryreset

Use this command to reset the configuration to the default settings for the currently installed firmware version.



Caution: Back up the configuration before proceeding. 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.

Syntax

```
config global
  execute factoryreset
```

Related topics

- [execute backup config](#)
- [execute em_dbbackup](#)
- [execute em_dbrestore](#)
- [execute restore config](#)
- [execute restore config-secure](#)
- [diagnose cmdb](#)

ping

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

Syntax

```
config global
  execute ping <address_ipv4>
```

Example

This example pings a host with the IP address 192.168.1.23.

```
config global
  execute ping 192.168.1.23
```

Related topics

- [execute ping-options](#)
- [execute traceroute](#)

ping-options

Use this command to set ICMP echo request (ping) options to control the way ping tests the network connection between the FortiScan appliance 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_ipv4>}
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_ipv4>}	Specify the FortiScan network interface from which to send the ping. If you specify auto, the FortiScan appliance selects the source address and interface based on the route to the <host-name_str> or <host_ipv4>. Specifying the IP address of a FortiScan network 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"> lowdelay = minimize delay throughput = maximize throughput reliability = maximize reliability lowcost = minimize cost default = 0 	default/ 0
ttl <hops_int>	Specify the time to live. Time to live is the number of hops the ping packet should be allowed to make before being discarded or returned.	64
validate-reply {yes no}	Select yes to validate reply data.	no
view-settings	Display the current ping-option settings.	No default.

Example

This command increases the number of pings sent.

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

Example

This example sends all pings from the FortiScan interface with IP address 192.168.10.23.

```
config global
execute ping-options source 192.168.10.23
```

Related topics

- [execute ping](#)

reboot

Use this command to restart the FortiScan appliance.

Syntax

```
config global
  execute reboot
```

Related topics

- [execute reload](#)
- [execute shutdown](#)

reload

Use this command to reload the FortiScan appliance's configuration.

Syntax

```
config global
  execute reload
```

Related topics

- [execute remove](#)
- [diagnose cmdb](#)

remove

Use this command to remove all reports.

Syntax

```
config global
  execute remove reports
```

reset_password

Use this command to reset the `admin` administrator account's password to the default password, `P@ssword1`.

Syntax

```
config global
  execute reset_password
```

restore config

Use this command to restore a plain text configuration file.



Caution: Back up the configuration before performing this procedure. This command will completely replace the appliance's configuration file, including administrator accounts and their passwords, and the current configuration will not be recoverable unless you have a complete configuration backup. For backup commands, see **both** “execute backup config” on page 64, and “execute em_dbbackup” on page 69.



Note: For a complete restoration, you must restore **both** the configuration file and the database. For the command to restore the configuration file, see “execute em_dbrestore” on page 71.

Syntax

```
config global
  execute restore config {ftp | sftp | scp | tftp} {<server_ipv4> |
    <server_fqdn>} <argument1_str> <argument2_str> <argument3_str>
    <argument4_str>
```

Variables	Description	Default
{ftp sftp scp tftp}	Choose which protocol to use to connect to the server. With SSH servers, use SCP.	No default.
{<server_ipv4> <server_fqdn>}	Type the IP address or domain name of the server. Note: Domain names are currently not valid input with this command if you choose the FTP protocol.	No default.
<argument1_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the user name that the FortiScan appliance will use to authenticate when connecting to the server. For TFTP, type the directory path on the server where the backup file is located. 	No default.
<argument2_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the password, if any. If there is no password, type a hyphen (-). For TFTP, type the file name of the backup. 	No default.
<argument3_str>	Type the directory path on the server where the backup was uploaded. This argument is not applicable when using the command with TFTP.	No default.
<argument4_str>	Type the file name of the backup.	No default.

Related topics

- [execute backup config](#)
- [execute em_dbrestore](#)
- [execute factoryreset](#)
- [execute ping](#)
- [execute restore config-secure](#)
- [diagnose cmdb](#)

restore config-secure

Use this command to restore an encrypted configuration file.



Caution: Back up the configuration before performing this procedure. This command will completely replace the appliance's configuration file, including administrator accounts and their passwords, and the current configuration will not be recoverable unless you have a complete configuration backup. For backup commands, see **both** “execute backup config-secure” on page 66, and “execute em_dbbackup” on page 69.



Note: For a complete restoration, you must restore **both** the configuration file and the database. For the command to restore the configuration file, see “execute em_dbrestore” on page 71.

Syntax

```
config global
  execute restore config-secure {ftp | sftp | scp | tftp} {<server_ipv4> |
  <server_fqdn>} <argument1_str> <argument2_str> <argument3_str>
  <argument4_str> <argument5_str>
```

Variables	Description	Default
{ftp sftp scp tftp}	Choose which protocol to use to connect to the server. With SSH servers, use SCP.	No default.
{<server_ipv4> <server_fqdn>}	Type the IP address or domain name of the server. Note: Domain names are currently not valid input with this command if you choose the FTP protocol.	No default.
<argument1_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the user name that the FortiScan appliance will use to authenticate when connecting to the server. For TFTP, type the directory path on the server where the backup is located. 	No default.
<argument2_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the password, if any. If there is no password, type a hyphen (-). For TFTP, type the file name of the backup. 	No default.
<argument3_str>	Type the directory path on the server where the backup was uploaded. This argument is not applicable when using the command with TFTP.	No default.
<argument4_str>	Type the file name of the backup.	No default.
<argument5_str>	Type the password that was used to encrypt the backup file.	No default.

Related topics

- [execute backup config-secure](#)
- [execute em_dbrestore](#)
- [execute factoryreset](#)
- [execute ping](#)
- [execute restore config](#)
- [diagnose cmdb](#)

restore image

Use this command to download a firmware image file that is located on a server. This command can be used to upgrade the appliance's firmware.



Caution: Back up the configuration before performing this procedure. This command can result in configuration changes required by the firmware version you are installing, and the current configuration will not be recoverable unless you have a complete configuration backup. For backup commands, see **both** “execute backup config” on page 64 or “execute backup config-secure” on page 66, and “execute em_dbbackup” on page 69.

Syntax

```
config global
  execute restore image {ftp | sftp | scp | tftp} {<server_ipv4> |
    <server_fqdn>} <argument1_str> <argument2_str> <argument3_str>
    <argument4_str>
```

Variables	Description	Default
{ftp sftp scp tftp}	Choose which protocol to use to connect to the server. With SSH servers, use SCP.	No default.
{<server_ipv4> <server_fqdn>}	Type the IP address or domain name of the server. Note: Domain names are currently <i>not</i> valid input with this command if you choose the FTP protocol.	No default.
<argument1_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the user name that the FortiScan appliance will use to authenticate when connecting to the server. For TFTP, type the directory path on the server where the firmware image is located. 	No default.
<argument2_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the password, if any. If there is no password, type a hyphen (-). For TFTP, type the file name of the firmware image. 	No default.
<argument3_str>	Type the directory path on the server where the firmware image was uploaded. This argument is not applicable when using the command with TFTP.	No default.
<argument4_str>	Type a file name for the firmware image.	No default.

Related topics

- [execute backup config](#)
- [execute backup config-secure](#)
- [execute em_dbbackup](#)
- [execute em_dbrestore](#)
- [execute factoryreset](#)
- [execute restore config](#)
- [execute restore config-secure](#)
- [execute ping](#)

restore vm

Use this command to install a FortiGuard Vulnerability Management Service (VCM) package that is stored on a server.



Caution: Back up the FortiGuard VCM package before beginning this procedure. The command will overwrite the existing package.

Syntax

```
config global
  execute restore vm {ftp | sftp | scp | tftp} {<server_ipv4> | <server_fqdn>}
    <argument1_str> <argument2_str> <argument3_str> <argument4_str>
```

Variables	Description	Default
{ftp sftp scp tftp}	Choose which protocol to use to connect to the server. With SSH servers, use SCP.	No default.
{<server_ipv4> <server_fqdn>}	Type the IP address or domain name of the server. Note: Domain names are currently <i>not</i> valid input with this command if you choose the FTP protocol.	No default.
<argument1_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the user name that the FortiScan appliance will use to authenticate when connecting to the server. For TFTP, type the directory path on the server where the FortiGuard package is located. 	No default.
<argument2_str>	Enter one of the following: <ul style="list-style-type: none"> For FTP, SFTP, or SCP, type the password, if any. If there is no password, type a hyphen (-). For TFTP, type the file name of the FortiGuard package. 	No default.
<argument3_str>	Type the directory path on the server where the FortiGuard package was uploaded. This argument is not applicable when using the command with TFTP.	No default.
<argument4_str>	Type a file name for the FortiGuard package.	No default.

Related topics

- [execute ping](#)
- [execute vm](#)
- [diagnose fortiguard](#)
- [diagnose vm status](#)
- [diagnose vm downgrade](#)
- [diagnose vm engine-log](#)
- [diagnose vm error-msg clear](#)
- [diagnose vm error-msg show](#)
- [diagnose vm error-msg upload](#)

set-date

Use this command to set the system date.

Syntax

```
config global
  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.

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

Related topics

- [execute set-time](#)
- [config system ntp](#)
- [config system global](#)

set-time

Use this command to set the system time.

Syntax

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

The variable <time_str> has the format 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 3:31:03 PM (15:31:03 using a 24-hour clock).

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

Related topics

- [execute set-date](#)
- [config system ntp](#)
- [config system global](#)

shutdown

Use this command to shut down the FortiScan appliance.

Syntax

```
config global
  execute shutdown
```

Related topics

- [execute reboot](#)

traceroute

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

Syntax

```
config global
  execute traceroute <host_ipv4>
```

Related topics

- [execute ping](#)

upload-benchmark

Use this command to upload benchmarks to the FortiScan appliance.

Syntax

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

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

Example

This example uploads 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
```

vm

Use this command to run vulnerability scan schedules and manage vulnerability reports.

Syntax

```
config adom
  edit <adom_name>
    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>
  end
end
```

Variable	Description	Default
<adom_name>	Type the name of the administrative domain (ADOM) whose vulnerability scans you want to configure.	No default.
map-config-run <map-config-name>	Enter to run a map configuration only one time.	
map-config-stop <map-config-name>	Enter to stop a running map configuration.	
report-clear <report-type [scan map]>	Enter to clear all scan or map reports.	
report-delete <report-type [scan <reportname> map <reportname>]	Enter to delete one report at a time.	
report-list <report-type [scan map]> <type> [name starttime endtime]	Enter to list all reports.	
schedule-run <schedule_name>	Enter to run a schedule one time.	
schedule-stop <schedule_name>	Enter to stop a running schedule.	

Example

This example runs a network vulnerability scan in the ADOM named CompanyA using the schedule named schedule_1.

```
config adom
  edit CompanyA
    execute vm schedule-run schedule_1
```

Related topics

- [config report output](#)

- config vm map-config
- config vm scan-profile
- config vm schedule
- config vm sensor
- diagnose fortiguard
- diagnose sys
- diagnose vm downgrade
- diagnose vm engine-log
- diagnose vm error-msg clear
- diagnose vm error-msg show
- diagnose vm error-msg upload
- diagnose vm status

get

`get` commands display a part of your FortiScan appliance'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:

```
global # get system dns

primary           : 172.1.1.5
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 appliance's CPU status, CPU usage, memory usage, and up time.

Syntax

```
config global
  get system performance
end
```

Example

This example displays the performance statistics of a FortiScan-3000C appliance:

```
global # 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
```

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 appliance's serial number
- the FortiBootloader ("BIOS") version
- FortiGuard Vulnerability and Compliance Management engine and plug-in version
- number of registered host asset IP addresses
- maximum number of host asset IP addresses allowed
- number of ADOMs
- hostname
- system time
- disk usage (and RAID status, if the appliance is a physical model such as FortiScan-3000C)
- license status

Syntax

```
config global
  get system status
end
```

Example

This example displays the various system statuses of a FortiScan-3000C appliance:

```
global # 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	

Example

This example shows output from FortiScan-VM:

```
FortiScan-VM # get system status
```

Output:

```
Version: FortiScan-VM v4.0,build0228,111021 (Interim)
Branch point: 228
Release Version Information: Interim
Serial-Number: FSC-VM0000000020
BIOS version: 04000002
VCM Service Pack: 2.075_1.234 [Thu Oct 20 19:13:00 2011]
The number of registered Compliance Assets: 11
Max Number of Compliance Host Asset Agents: 20000
Admin Domain Status: enabled
Number of Admin Domain: 2
Max number of administrative domains: 200
Hostname: FortiScan-VM
FIPS mode: disabled
System Time: Thu Oct 27 08:50:17 PDT 2011

Disk Usage: Free 19.27GB, Total 29.53GB
License Status: Invalid
```

Related topics

- [get system performance](#)
- [config system raid](#)
- [config system ntp](#)
- [execute set-date](#)
- [execute set-time](#)
- [execute restore config](#)
- [execute vm](#)
- [diagnose sys](#)

diagnose

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



Note: All diagnose commands are global in scope, and are only available from within `config global`.

This chapter contains the following sections:

diagnose alertmail error-msg	diagnose debug info	diagnose raid
diagnose cmdb	diagnose debug output	diagnose sniffer packet
diagnose debug application	diagnose debug report	diagnose sys
diagnose debug capture-output	diagnose debug reset	diagnose vm downgrade
diagnose debug cli	diagnose debug timestamp	diagnose vm engine-log
diagnose debug crashlog	diagnose fortiguard	diagnose vm error-msg clear
diagnose debug dbsync	diagnose gui console	diagnose vm error-msg show
diagnose debug emdb	diagnose netlink	diagnose vm error-msg upload
diagnose debug emserver	diagnose ntpd	diagnose vm status

alertmail error-msg

Use this command to manage alert mail daemon error messages.

Syntax

```
config global
  diagnose alertmail error-msg {clear | show | upload <ftp_ipv4>}
```

Variable	Description	Default
{clear show upload <ftp_ipv4>}	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_ipv4>.	No default.

Example

This example displays recent alert email daemon error messages:

```
config global
  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
```

Related topics

- [config system mail](#) (in config global)
- [config system mail](#) (in config adom)

cmdb

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

Syntax

```
config global
  diagnose cmdb cmdb-profile {info | node <path.object[.attribute]>}
  diagnose cmdb error-msg {clear | show | upload <ftp_ipv4>}
```

Variable	Description	Default
cmdb-profile {info node <path.object[.attribute]>}	Display CMDB profile shared memory information, or CMDB profile by node.	No default.
error-msg {clear show upload <ftp_ipv4>}	clear - Removes alert CMDB error messages. show - Displays recent CMDB error messages. upload - Save the CMDB error messages to an FTP server.	No default.

Example

This example uploads the CMDB error messages to an FTP server.

```
config global
  diagnose cmdb error-msg upload 192.168.10.1
```

Related topics

- [execute backup config](#)
- [execute factoryreset](#)
- [execute reload](#)
- [execute restore config](#)
- [execute restore vm](#)

debug application

Use this command to set the level of detail in the debug log for the FortiScan applications.

Syntax

```
config global
  diagnose debug application alert <debug_level_int>
  diagnose debug application alertmail <debug_level_int>
  diagnose debug application cmdb <debug_level_int>
  diagnose debug application fnbamd <debug_level_int>
  diagnose debug application fortiguard <debug_level_int>
  diagnose debug application miglogd <debug_level_int>
  diagnose debug application network-summary <debug_level_int>
  diagnose debug application ntpd <debug_level_int>
  diagnose debug application remote-auth <debug_level_int>
  diagnose debug application snmpd <debug_level_int>
  diagnose debug application uploadd <debug_level_int>
  diagnose debug application vm <debug_level_int>}
```

Variable	Description	Default
alert <debug_level_int>	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_int>	Set the debug level of alert email daemon from 0-8.	0
cmdb <debug_level_int>	Set the debug level of FortiScan Web Services from 0-8.	0
fnbamd <debug_level_int>	Set the debug level of the Fortinet authentication daemon from 0-8.	0
fortiguard <debug_level_int>	Set the debug level of the FortiGuard daemon from 0-8.	0
miglogd <debug_level_int>	Set the debug level of the miglog daemon from 0-8.	0
network-summary <debug_level_int>	Set the debug level of the network summary daemon from 0-8.	0
ntpd <debug_level_int>	Set the debug level of the Network Time Protocol (NTP) daemon from 0-8.	0
remote-auth <debug_level_int>	Set the debug level of the remote authentication daemon from 0-8.	0
snmpd <debug_level_int>	Set the debug level of the SNMP daemon from 0-8.	0
uploadd <debug_level_int>	Set the debug level of upload daemon from 0-8.	0
vm <debug_level_int>	Set the debug level of vulnerability management daemon from 0-8.	0

Example

This sets the debug level to 5 for the vulnerability management daemon.

```
config global
  diagnose debug application vm 5
```

Related topics

- [diagnose debug cli](#)
- [diagnose debug crashlog](#)

debug capture-output

Use this command to set capture output type.

Syntax

```
config global
  diagnose debug capture-output {clear|disable|enable|show|upload <ftp_ipv4>}
```

Variable	Description	Default
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_ipv4>	Save the capture output file to an FTP server.	

Example

This example uploads the capture output file to an FTP server.

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

debug cli

Use this command to set the debug level of CLI.

Syntax

```
config global
  diagnose debug cli <integer>
```

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

Example

This example sets the CLI debug level to 5.

```
config global
  diagnose debug cli 5
```

Related topics

- [diagnose debug application](#)

debug crashlog

Use this command to display, upload, and delete crash logs.

Syntax

```
config global
  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	Default
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 lists applications that have backtraces or core files:

```
config global
  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
```

Related topics

- [diagnose debug application](#)
- [diagnose debug dbsync](#)
- [diagnose debug emdb](#)

debug dbsync

Use this command to view internal FortiScan database synchronization logs.

Internally, each FortiScan appliance has two PostgreSQL databases: the master database and the slave database. The watchdog monitors the two databases to ensure that they continuously synchronize. Watchdog logs shows the databases' synchronization status and history.

Syntax

```
config global
  diagnose debug dbsync listlogs {master | slave | watchdog}
  diagnose debug dbsync loghist {master | slave} '<from_str>' '<to_str>'
  diagnose debug dbsync logrt {master | slave | watchdog} <log-file_name>
  diagnose debug dbsync readlog {master | slave | watchdog} <log-file_name>
  diagnose debug dbsync upload {ftp | sftp | scp | tftp} <address_ipv4>
    <arg1_str> <arg2_str> <arg3_str> <arg4_str>
```

Variable	Description	Default
listlogs {master slave watchdog}	List all available logs for the master database, slave database, and watchdog. The log file names can be used with the diagnose debug dbsync logrt {master slave watchdog} <log-file_name> command.	
loghist {master slave} '<from_str>' '<to_str>'	Display master or slave database logs within a specific time range. Both <from_str> (the start of the range) and <to_str> (the end of the range) are in the format: yyyy-mm-dd hh:mm:ss	
logrt {master slave watchdog} <log-file_name>	Display a database synchronization log file for the master database, slave database, or watchdog, and continuously update the display as log entries are added to the file in real time.	
readlog {master slave watchdog} <log-file_name>	Display a database synchronization log file for the master database, slave database, or watchdog. Unlike diagnose debug dbsync logrt {master slave watchdog} <log-file_name>, this command does not update the display as log entries are added. To view new logs, you must repeat the command.	
upload {ftp sftp scp tftp} <address_ipv4> <arg1_str> <arg2_str> <arg3_str> <arg4_str>	Upload a log file to an FTP, SFTP, SCP, or TFTP server, where: <ul style="list-style-type: none"> • <address_ipv4> – Type the IP address or, for any protocol except FTP, the domain name of the server. • <arg1_str> – For FTP, SFTP, or SCP, type the user name that the FortiScan appliance will use to connect to the server. For TFTP, type a directory or file name. • <arg2_str> – For FTP, SFTP, or SCP, type the password corresponding to the user name, or, if there is none, enter a hyphen (-). For TFTP, type the file name or press Enter. • <arg3_str> – For FTP, SFTP, or SCP, type the directory or name of the log file when it is uploaded to the server. For TFTP, press Enter. • <arg4_str> – Enter a file name or press Enter. 	

Example

This example lists master database synchronization logs:

```
config global
  diagnose debug dbsync listlogs master
```

Output:

```
em_db-2011-02-18_00:50:13.log: 387955 bytes, Mon Mar 7 09:41:52 PST 2011
```

```
em_db-2011-03-07_17:54:24.log: 914118 bytes, Mon Apr 18 13:41:40 PDT 2011
em_db-2011-04-18_21:00:30.log: 196773 bytes, Wed Apr 27 10:18:10 PDT 2011
em_db-2011-04-27_17:31:23.log: 118797 bytes, Mon May 2 16:09:31 PDT 2011
em_db-2011-05-02_23:22:08.log: 5747 bytes, Mon May 2 16:26:47 PDT 2011
em_db-2011-05-02_23:43:17.log: 21498 bytes, Tue May 3 10:08:03 PDT 2011
em_db-2011-05-03_17:11:26.log: 160164 bytes, Tue May 10 14:07:10 PDT 2011
em_db-2011-05-10_21:10:39.log: 5923 bytes, Tue May 10 14:41:59 PDT 2011
em_db-2011-05-10_21:45:15.log: 176112 bytes, Wed May 18 09:28:48 PDT 2011
```

Related topics

- [diagnose debug emdb](#)

debug emdb

Use this command to view FortiScan database logs.

Syntax

```
config global
  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	Default
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"> • <address_ipv4> – The IP address of the server. • <arg_1> – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename. • <arg_2> – For FTP, SFTP or SCP enter a password or enter ‘.’. For TFTP enter the filename or press Enter. • <arg_3> – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter. • <arg_4> – Enter a filename or press Enter. Note: Use the FTP server’s IP address whenever you are entering the FTP server information. Using a domain name is not supported.	

Example

This example lists the appliance’s system database logs:

```
config global
  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
```

Related topics

- [diagnose debug emserver](#)

debug emserver

Use this command to view FortiScan system logs.

Syntax

```
config global
  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	Default
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"> • <address_ipv4> – The server IP address • <arg_1> – For FTP, SFTP or SCP enter a user name. For TFTP enter a directory or filename. • <arg_2> – For FTP, SFTP or SCP enter a password or enter '-'. For TFTP enter the filename or press Enter. • <arg_3> – For FTP, SFTP or SCP enter a directory or filename. For TFTP, press Enter. • <arg_4> – Enter a filename or press Enter. <p>Note: 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 lists the appliance's event logs:

```
config global
  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
```

Related topics

- [diagnose debug emdb](#)

debug info

Use this command to show active debug level settings.

Syntax

```
config global
  diagnose debug info
```

debug output

Use this command to enable debug output.

Syntax

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

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

Example

This example shows how to enable the debug output:

```
config global
  diagnose debug output enable
```

Related topics

- [diagnose debug application](#)
- [diagnose debug capture-output](#)
- [diagnose debug info](#)
- [diagnose debug reset](#)
- [diagnose debug timestamp](#)

debug report

Use this command to display the FortiScan configuration.

Syntax

```
config global
  diagnose debug report
```

debug reset

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

Syntax

```
config global
  diagnose debug reset
```

Related topics

- [diagnose debug application](#)

debug timestamp

Use this command to enable or disable debug timestamp.

Syntax

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

Related topics

- [diagnose debug output](#)

fortiguard

Use this command to manage the FortiGuard daemon, which handles connections to the FortiGuard Distribution Network (FDN).

Syntax

```
config global
  diagnose fortiguard {error-msg {clear | show | upload <ftp_ipv4>} | status |
    vm-refresh}
```

Variable	Description	Default
error-msg {clear show upload <ftp_ipv4>}	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 FortiGuard Distribution Network status. This process may take a few minutes.	

Example

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

```
config global
  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
```

Related topics

- [execute restore vm](#)
- [execute vm](#)

gui console

Use this command to check the status of the web UI.

Syntax

```
config global
  diagnose gui console
```

Related topics

- [config system global](#)

netlink

Use this command to display network link, session, and routing information.

Syntax

```
config global
  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	Default
device list	Display the FortiScan appliance's interface statistics.	
interface list	Display the FortiScan appliance's interface status and parameters.	
ip list	Display all of the physical and virtual IP addresses associated with the network interfaces of the FortiScan appliance.	
route list	Display the FortiScan appliance's routing table contents.	
rtcache list	Display the FortiScan appliance's routing cache information.	
tcp list	Display the FortiScan appliance's TCP socket information.	
udp list	Display the FortiScan appliance's UDP sockets information.	

Example

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

```
config global
  diagnose netlink interface list
```

Output:

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

flags=noarp

Related topics

- [config system interface](#)
- [config system route](#)

ntp

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

Syntax

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

Variable	Description	Default
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:

```
config global
  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
```

Related topics

- [config system ntp](#)
- [config system dns](#)

raid

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

Syntax

```
config global
  diagnose raid delete <disk_int>}
  diagnose raid info
```

Variable	Description	Default
delete <disk_int>}	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.	No default.

Example

This example shows how to list the RAID information on a FortiScan-3000C Appliance:

```
config global
  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
```

Related topics

- [config system raid](#)
- [get system status](#)

sniffer packet

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 appliance, 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

```
config global
  diagnose sniffer packet [<interface_name>] [{none | '<filter_str>'}] [{1 | 2
  | 3}] [<count_int>]
```

Variable	Description	Default
[<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.	No default.
[{none '<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 {<host1_fqdn> <host1_ipv4>}] [and or] [[src dst] host {<host2_fqdn> <host2_ipv4>}] [and or] [[arp ip gre esp udp tcp] port <port1_int>] [and or] [[arp ip gre esp udp tcp] port <port2_int>]'</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>	none
[{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"> • 1 for header only • 2 for IP header and payload • 3 for Ethernet header and payload For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (3).	1
[<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.	Packet capture continues until you press Ctrl + C.

Example

This 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`).

Commands that you would type are highlighted in bold; responses from the FortiScan appliance are not bolded.

```
FortiScan# config global
FortiScan# 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

This 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 appliance are not bolded.

```
FortiScan# config global
FortiScan# 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

This 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 appliance are not bolded.

```

FortiScan# config global
FortiScan# 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 PuTTY or Microsoft HyperTerminal to save the sniffer output. Methods may vary. See the documentation for your CLI client.

Requirements

- terminal emulation software such as [PuTTY](#)
- a plain text editor such as Notepad
- a [Perl](#) interpreter
- network protocol analyzer software such as [Wireshark](#)

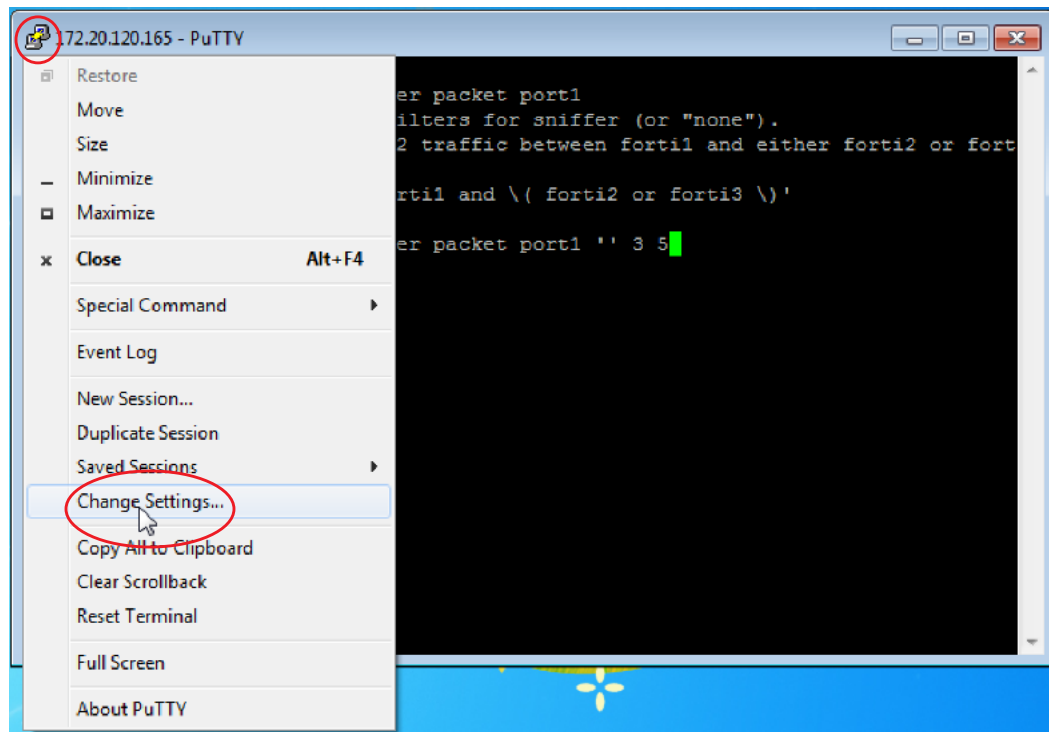
To view packet capture output using PuTTY and Wireshark

- 1 On your management computer, start PuTTY.
- 2 Use PuTTY to connect to the FortiScan appliance using either a local serial console, SSH, or Telnet connection. For details, see “[Connecting to the CLI](#)” on page 17.
- 3 Type the packet capture command, such as:

```
diag sniffer packet port1 'tcp port 443' 3 100
```

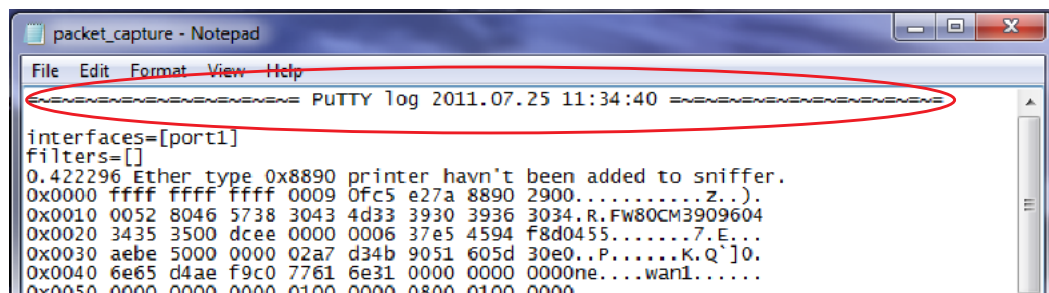
but do **not** press Enter. yet

- In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select *Change Settings*.



A dialog appears where you can configure PuTTY to save output to a plain text file.

- In the *Category* tree on the left, go to *Session > Logging*.
- In *Session logging*, select *Printable output*.
- In *Log file name*, click the *Browse* button, then choose a directory path and file name such as `C:\Users\MyAccount\packet_capture.txt` to save the packet capture to a plain text file. (You do not need to save it with the `.log` file extension.)
- Click *Apply*.
- Press Enter to send the CLI command to the FortiMail unit, beginning packet capture.
- If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press `Ctrl + C` to stop the capture.
- Close the PuTTY window.
- Open the packet capture file using a plain text editor such as Notepad.



- Delete the first and last lines, which look like this:

```

===== PuTTY log 2011.07.25 11:34:40
=====
FortiScan-2000 #

```

These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.

14 Convert the 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.

To use fgt2eth.pl, open a command prompt, then enter a command such as the following:



Note: Methods to open a command prompt vary by operating system.

On Windows XP, go to *Start > Run* and enter `cmd`.

On Windows 7, click the Start (Windows logo) menu to open it, then enter `cmd`.

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.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
- `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `packet_capture.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

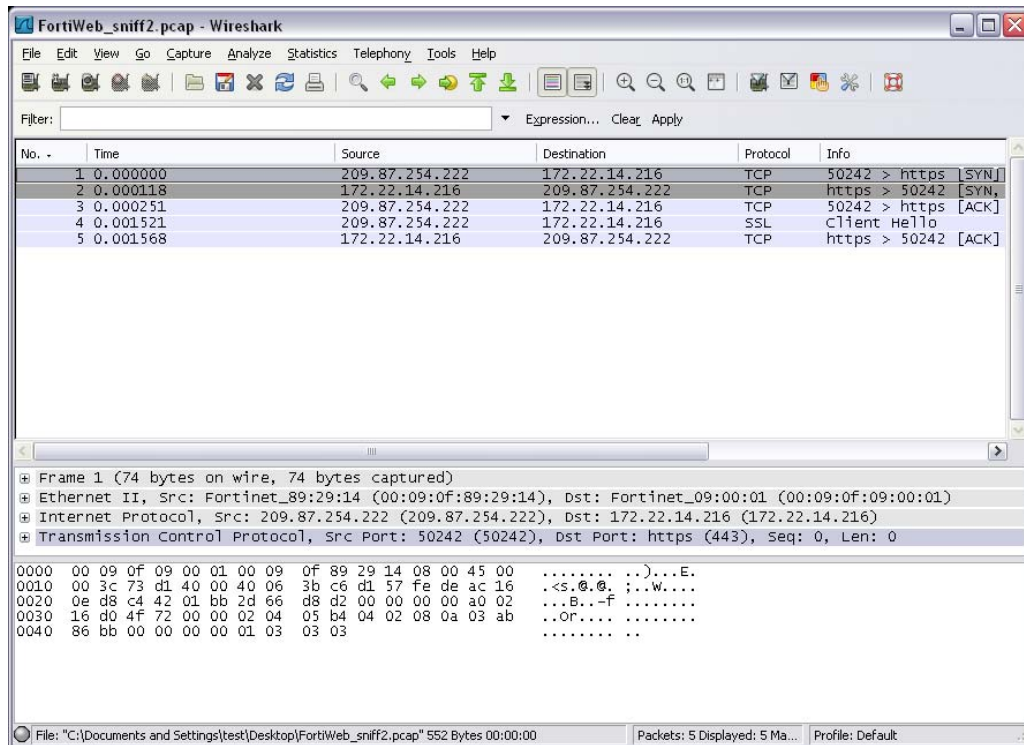
C:\Documents and Settings\test\Desktop>fgt2eth.pl -in FortiWeb_sniff.txt -out FortiWeb_sniff.pcap
Conversion of file FortiWeb_sniff.txt phase 1 (FGI verbose 3 conversion)
Output written to FortiWeb_sniff.pcap.
Conversion of file FortiWeb_sniff.txt phase 2 (windows text2pcap)
Output file to load in Ethereal is 'FortiWeb_sniff.pcap'

C:\Documents and Settings\test\Desktop>

```

15 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](#).

Related topics

- [config system interface](#)

sys

Use this command to view and manage the system information.

Syntax

```
config global
  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	Default
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 appliance and each of the registered devices.	

Variable	Description	Default
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 fsfix 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 fscheck, fsfix, and fsrebuild commands.</p> <p>reset-mount-count - Set the mount-count of log disk to 1 upon system reboot.</p>	
fsystem	Display the log disk file system information.	
interface <port>	Display the detailed information for an interface.	
kill <signal> <pid>	Send a signal to terminate a process that is currently running on the system. <ul style="list-style-type: none"> • <signal> - the signal number to send. • <pid> - the process ID where the signal is sent to. 	
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>	Display the top processes. <value> - the refreshing interval in seconds. The default is 5.	

Example

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

```
config global
  diagnose system 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
```

Related topics

- [get system status](#)

vm downgrade

Use this command to enable or disable downgrading of the vulnerability management (VM) engine.

Syntax

```
config global
  diagnose vm downgrade [{enable | disable}]
```

Variable	Description	Default
[{enable disable}]	Enable or disable downgrading the VM engine. To determine whether or not VM engine downgrades are currently enabled, enter <code>diagnose vm downgrade</code> (without the trailing <code>enable</code> or <code>disable</code> word).	disable

Example

This example enables VM engine downgrades, and then verifies the setting.

```
config global
  diagnose vm downgrade enable
  diagnose vm downgrade
```

Output:

```
VM engine downgrade is currently enabled.
```

Related topics

- [execute vm](#)
- [execute restore vm](#)

vm engine-log

Use this command to display logs for the vulnerability management (VM) daemon.

Syntax

```
config global
  diagnose vm engine-log
```

Related topics

- [execute vm](#)

vm error-msg clear

Use this command to delete error messages from the vulnerability management (VM) daemon.

Syntax

```
config global
  diagnose vm error-msg clear
```

Related topics

- [execute vm](#)

vm error-msg show

Use this command to display error messages from the vulnerability management (VM) daemon.

Syntax

```
config global
  diagnose vm error-msg show
```

Example

This example displays two error messages from the VM daemon:

```
config global
  diagnose vm status
```

Output:

```
[2011-02-17 16:58:14] ERROR: vm(1452):rvsagent.c:460: create trend dbtable
error:(null)
[2011-02-17 16:49:33] ERROR: vm(564):rvsagent.c:460: create trend dbtable
error:(null)
```

Related topics

- [execute vm](#)

vm error-msg upload

Use this command to upload error messages from the vulnerability management (VM) daemon to an FTP server.

Syntax

```
config global
  diagnose vm error-msg upload <ftp-server_ipv4> <directory_str> <user_str>
    <password_str>
```

Variable	Description	Default
<ftp-server_ipv4>	Type the IP address of an FTP server where you want to upload the error messages.	No default.
<directory_str>	Type the directory path, relative to the service's root folder, on the FTP server where you want to upload the error messages.	No default.
<user_str>	Type the user name of an account on the FTP server that the appliance can use to authenticate when it uploads.	No default.
<password_str>	Type the password associated with the user name.	No default.

Example

This example uploads VM daemon error messages to the `tmp` folder on an FTP server at the IP address 172.1.1.10.

```
config global
  diagnose vm error-msg upload 172.1.1.10 tmp user1 P@55w0rd1
```

Output:

```
Compress following files to vm.dbg.tgz to prepare for uploading.
vm.dbg
```

```
Upload request of vm.dbg.tgz to ftp://172.1.1.10/tmp succeeded.
```

Related topics

- [execute vm](#)

vm status

Use this command to display the queue status of the vulnerability management (VM) daemon.

Syntax

```
config global
  diagnose vm status
```

Example

This example shows the running status of the VM daemon:

```
config global
  diagnose vm status
```

Output:

```
Currently no running schedule.
Scan schedule(s) queued:
    None.
Map schedule(s) queued:
    None.
Compliance jobs:
    None.
```

Related topics

- [execute vm](#)

show

The `show` commands display a part of your FortiScan appliance'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:

```
global # config global
global # show system dns

config system dns
    set primary 172.1.1.5
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, 24
 _fqdn, 24
 _index, 24
 _int, 24
 _ipv4, 24
 _ipv4/mask, 24
 _ipv4mask, 24
 _ipv4range, 24
 _name, 24
 _pattern, 24
 _str, 24
 _v4mask, 24

A

abort, 27
 administrator
 admin, 18
 ambiguous command, 22, 28
 ASCII, 29
 auto-negotiation, 41

B

batch changes, 17, 30
 baud rate, 30
 bits per second (bps), 18
 boot interrupt, 17
 buffer, terminal emulator, 30

C

certification, 12
 characters, special, 28
 classless inter-domain routing (CIDR), 24
 CLI Console widget, 19
 command, 22
 abbreviation, 28
 ambiguous, 22, 28
 completion, 28
 constraints, 14
 help, 28
 incomplete, 23
 interactive, 28
 multi-line, 22, 28
 prompt, 25, 28, 30
 scope, 22, 23
 command line interface (CLI), 12, 14, 22
 connecting, 17
 comments, 12

Configuration Management Database (CMDB), 99
 configuration script, 17
 console port, 17, 18
 conventions, 13
 CPU status, 94
 CPU usage, 94

D

data-size, 75
 DB-9, 18
 default
 administrator account, 18
 password, 12, 18
 definitions, 22
 df-bit, 75
 diagnose
 alertmail, 98
 cmdb, 99
 debug application, 100
 debug capture-output, 102
 debug CLI, 103
 debug crashlog, 104
 debug emdb, 108, 109
 debug info, 111
 debug output, 112
 debug report, 113
 debug reset, 114
 debug timestamp, 115
 fortiguard, 116
 gui, 117
 netlink, 118
 ntpd, 120
 raid, 121
 sys, 130
 vm downgrade, 133
 vm engine-log, 134
 vm error-msg clear, 135
 vm error-msg show, 136
 vm error-msg upload, 137
 vm status, 138
 documentation, 12
 commenting on, 12
 domain name, 39
 dotted decimal, 24
 duplex, 41

E

encoding, 29
 error message, 23
 escape sequence, 28

execute
 backup config, 64
 backup config-secure, 66
 disconnect, 68
 factoryreset, 73
 ping, 74
 ping-options, 75
 reboot, 77
 reload, 78
 restore config, 81
 restore config-secure, 82
 restore image, 83
 restore vm, 84
 set-date, 85
 set-time, 86
 shutdown, 87
 update-vm, 89
 vm, 90

execute command
 ping, 74, 88
 restore, 88

expected input, 14, 22

exploit, 11

F

factoryreset, execute, 73

FAQ, 12

field, 23

firmware
 restoring, 17

flow control, 18

font, 29

FortiGuard
 services, 11
 Vulnerability Management Service, 12

Fortinet
 customer service, 11
 Knowledge Base, 12
 Technical Documentation, 12
 Technical Support, 11, 124
 Technical Support, registering with, 11
 Technical Support, web site, 11
 Training Services, 12

fully qualified domain name (FQDN), 24

H

host name, 39

how-to, 12

I

idle timeout, 39

incomplete command, 23

indentation, 23

index number, 24

input constraints, 14, 22

installation, 12

K

key, 21

Knowledge Base, 12

L

language, 29, 39

line endings, 30

link speed, 41

local console access, 17

login prompt, 18

M

maximum transmission unit (MTU), 40

memory usage, 94

more, 30

multi-line command, 22, 28

multiple pages, 30

N

no object in the end, 23

null modem, 18, 19

O

object, 23

option, 23

P

packet
 capture, 124
 trace, 124

paging, 30

parity, 18

password, 18
 administrator, 12

pattern, 24

pattern, ping-options, 75

peer connection, 19

ping, execute, 74, 88

ping-options, execute, 75

plain text editor, 30

product registration, 11

R

registering
 with Fortinet Technical Support, 11

regular expression, 24

repeat-count, 75

report
 output, 50

reserved characters, 28

restore, execute, 88

restoring the firmware, 17

RFC
 1918, 13

risk, 11

RJ-45, 18, 19

RJ-45-to-DB-9, 18, 19

route, 45

S

- Secure Shell (SSH), 17, 20
 - key, 21
- serial communications (COM) port, 18, 19
- sniffer, 124
- source, ping-options, 75
- special characters, 28, 29
- speed, 41
- SSH, 19, 20
 - key, 21
- string, 24
- sub-command, 22, 23, 25
- syntax, 14, 22
- system
 - console, 35
 - fortiguard, 37
 - global, 39
 - interface, 40
 - mail, 42, 52
 - ntp, 43
 - raid, 44
 - route, 45
 - snmp, 46

T

- table, 23
- technical
 - documentation, 12
 - support, 11

- Telnet, 17, 19, 20, 21
- time zone, 39
- timeout, 39
- timeout, ping-options, 75
- tips and tricks, 27
- tos, 75
- Training Services, 12
- troubleshooting, 97, 124
 - can't connect to the web UI, 72
- ttl, 75

U

- unknown action, 22
- up time, 94
- US-ASCII, 29, 126

V

- validate-reply, 75
- value, 23
- value parse error, 23, 24
- view-settings, 75

W

- wild cards, 24

Z

- zero-day vulnerabilities, 11

FORTINET[®]

www.fortinet.com