

# Juniper Advanced Threat Prevention Appliance

## CLI Command Reference Guide

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA

408-745-2000

[www.juniper.net](http://www.juniper.net)

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Advanced Threat Prevention CLI Command Reference Guide  
Copyright© 2018 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical document consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# CONTENTS

## About the Documentation

Documentation and Release Notes .....	vii
Requesting Technical Support .....	vii
Self-Help Online Tools and Resources .....	vii
Opening a Case with JTAC .....	viii

## Preface

About This Guide .....	1
Organization .....	1
Typographical Conventions .....	2
Related Documentation .....	2

## Introduction

Accessing the CLI .....	3
Hardware Appliance Access via the Console .....	3
Configuration Wizard Command Prompt Progressions .....	4
Hardware, Software and Virtual Appliance Access via SSH .....	6
CLI Help and Keyboard Shortcuts .....	6
CLI Modes .....	7

## All-in-One CLI Commands

Basic Mode Commands .....	9
CM Commands .....	10
Core Mode Commands .....	10
Server Mode Commands .....	10
Collector Mode Commands .....	10
Diagnosis Mode Commands .....	11
All-in-One CLI Commands .....	11
capture-start .....	11
cm .....	12
collector .....	12
copy .....	13
core .....	13
diagnosis .....	14
exit .....	14
gssreport .....	15
help .....	16
history .....	17
ifrestart .....	17
ping .....	18
reboot .....	18
restart .....	19
restore .....	20

server	20
set honeypot (collector mode)	22
set traffic-monitoring (for JATP700 Appliances only) (collector mode)	22
set traffic-filter (collector mode)	23
set protocols (collector mode)	23
set proxy (collector mode)	24
set (diagnosis mode)	25
set ip interface (server mode)	26
set (server mode)	27
set system-alert (server mode)	29
setupcheck	30
show (collector mode)	31
show (core mode)	32
show (diagnosis mode)	33
shutdown	34
traceroute	34
upgrade	34
updateimage	35
wizard	35
Configuration Wizard for the All-in-One Server	36

## Core/CM Server CLI Commands

Basic Mode Commands	37
CM Commands	37
Core Mode Commands	38
Server Mode Commands	38
Diagnosis Mode Commands	38
CoreCM CLI Commands	39
capture-start	39
cm	39
core	40
copy	41
diagnosis	41
exit	42
gssreport	42
help	43
history	44
ifrestart	44
ping	45
reboot	45
restart	45
restore	47
set (core mode)	48
server	48
set system-alert (server mode)	48
set (server mode)	50
set (diagnosis mode)	52

setupcheck .....	52
show (core mode) .....	53
show (server mode) .....	55
shutdown .....	58
traceroute .....	58
upgrade .....	58
updateimage .....	59
wizard .....	59
Configuration Wizard for the CoreCM Server .....	60
<b>Mac OS X Engine CLI Commands</b>	
Basic Mode Commands .....	63
Core Mode Commands .....	63
Server Mode Commands .....	64
Diagnosis Mode Commands .....	64
Mac OS X Detection Engine CLI Commands .....	65
capture-start .....	65
copy .....	65
core .....	66
diagnosis .....	66
exit .....	67
gssreport .....	67
help .....	68
history .....	69
ifrestart .....	69
ping .....	70
reboot .....	70
restart .....	70
restore .....	72
server .....	72
set (server mode) .....	74
set (diagnosis mode) .....	76
setupcheck .....	77
show (core mode) .....	77
show (diagnosis mode) .....	78
show (server mode) .....	79
shutdown .....	81
traceroute .....	81
updateimage .....	81
upgrade .....	83
wizard .....	83
Configuration Wizard Command Prompt Responses .....	84
<b>Traffic Collector CLI Commands</b>	
Basic Mode Commands .....	87
Collector Mode Commands .....	87
Diagnosis Mode Commands .....	88
Server Mode Commands .....	88

Traffic Collector CLI Commands .....	89
capture-start .....	89
collector .....	89
copy .....	90
diagnosis .....	90
exit .....	91
gssreport .....	91
help .....	92
history .....	93
ifrestart .....	93
ping .....	94
reboot .....	94
restart .....	94
restore .....	96
server .....	97
set proxy (collector mode) .....	97
set honeypot (collector mode) .....	98
set (diagnosis mode) .....	99
set protocols (collector mode) .....	99
set (server mode) .....	100
set traffic-filter (collector mode) .....	102
set traffic-monitoring (for JATP700 Appliances only) (collector mode) .....	102
setupcheck .....	103
show (collector mode) .....	104
show (diagnosis mode) .....	105
show (server mode) .....	106
shutdown .....	108
tracertoute .....	108
wizard .....	108
Configuration Wizard Command Prompt Progressions .....	109

## Glossary of Terms

# About the Documentation

## Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes. Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>.
- Search for known bugs: <https://prsearch.juniper.net/>.
- Find product documentation: <http://www.juniper.net/documentation/>.
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>.
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>.
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>.
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>.
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>.

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>.

### Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).
- For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>



# Preface

This preface contains the following sections:

- [About This Guide on page 1](#)
- [Organization on page 1](#)
- [Typographical Conventions on page 2](#)
- [Related Documentation on page 2](#)

## About This Guide

This guide describes the commands that make up the command-line interface (CLI) of the Juniper ATP Appliance.

This guide is intended for system administrators responsible for deploying, operating, and maintaining the Juniper ATP Appliance.

## Organization

This guide is organized as follows:

- Chapter 1, “Introduction”—Includes an overview of CLI usage, CLI Modes and information about how to access the Juniper ATP Appliance Command Line Interface.
- Chapter 2, “All-in-One CLI Commands”—Provides information about system commands for updating the product boot images, setting configurations, and defining system-level settings for Collector and Detection Engine interfaces and network deployment services.
- Chapter 3, “Core/CM Server CLI Commands”—Provides information about commands available to the Core and Central Manager for all hardware appliance, software appliance, and virtual appliance models, including the commands used to manage Detection Engines and Juniper ATP Appliance system configuration.
- Chapter 4, “Mac OS X Engine CLI Commands”—Provides information about Mac Mini Mac OS X Detection Engine-specific commands for configuration and status monitoring.
- Chapter 5, “Traffic Collector CLI Commands”—Provides information about the Juniper ATP Appliance Traffic Collector commands available for identifying, monitoring, and configuring distributed Collector hardware, software and virtual appliances.
- Chapter 6, “Glossary of Terms”—Provides a set Juniper ATP Appliance-specific as well as cybersecurity industry terms and definitions.

## Typographical Conventions

This guide uses the following typographical conventions for special terms and instructions.

Table 4-1 Typographical Conventions

Convention	Meaning	Example
courier font	Coding examples and text to be entered at the command prompt	Enter the following command: server set dns
Click	A left-mouse button click.	Click Download IVP to perform endpoint infection verification.
Double-click	A double-click of the left mouse button.	Double-click the report name to open in the integrated SIEM application.
Right-click	A right mouse button click.	Right-click on the icon to view its properties.
<   > (text in angle brackets; items separated by the pipe symbols)	Option for selection of required parameter and/or value.	interfaces set stp <on   off >
[ ] (text in square brackets) or [   ] (text in square brackets, items separated by pipe symbols)	Optional parameters and values, with selection options separated by the pipe symbol.	show device alarm [cpu_util   paging]

## Related Documentation

The following is a list of additional Juniper ATP Appliance documentation:

- Juniper ATP Appliance Release Notes— Describes the latest release of the Juniper ATP Appliance software.
- Juniper ATP Appliance Quick Start Guides— Quick Starts describe how to install and initially configure a Juniper ATP Appliance; refer to the Quick Start for your device or model.
- Juniper ATP Appliance Operator's Guide— The Operator's Guide describes usage of all aspect of the Juniper ATP Appliance All-in-One or distributed defense system.
- Juniper ATP Appliance CEF/SYSLOG Support for SIEM — This guide provides information about Juniper ATP Appliance CEF and Syslog Logging for SIEM.
- Juniper ATP Appliance Safety and Regulatory Guide—Contains conformance and safety information for Juniper ATP Appliances.
- Juniper ATP Appliance API Reference Guide— Provides Juniper ATP Appliance HTTP API functions and information about usage.

## CHAPTER 1

# Introduction

This chapter explains how to use the Juniper ATP Appliance command line interface (CLI) to configure and administer a Juniper ATP Appliance.

This chapter contains the following sections:

- “Accessing the CLI” in the next section
- CLI Help and Keyboard Shortcuts on page 16
- CLI Modes on page 17

### Accessing the CLI

You have the option of accessing the Juniper ATP Appliance CLI in either of two ways:

- Console
- SSH

---

**NOTE** Always use the latest version of Putty for SSH operations, if using Putty as an SSH client.

---

### Hardware Appliance Access via the Console

To access the Juniper ATP Appliance CLI using the console port:

1. Connect your computer's serial port to the DB-9 console port on the Juniper ATP Appliance.
2. Open a terminal program such as Console on Mac OS X, HyperTerminal on Windows, or Minicom on Linux.
3. Configure the terminal program serial communication settings as follows:
  - › Bits per second: 960
  - › Data bits: 8
  - › Stop bit: 1
  - › Parity: None
4. At the CLI prompt, enter your username and password. By default, the admin user name is **admin** and the password is **1JATP234**.

Be sure to change the default password for the admin account after initial setup; the password must be at least 8 characters in length.

5. To launch the configuration wizard, enter the command `wizard`.

```
# wizard
```

## Configuration Wizard Command Prompt Progressions

**NOTE** Enter CTRL-C to exit the Configuration Wizard at any time. If you exit without completing the configuration, you will be prompted again whether to run the Configuration Wizard.

You may also rerun the Configuration Wizard at any time with the CLI command **wizard**.

Configuration Wizard Prompts	Customer Response from <u>All-in-One</u>	Customer Response from <u>Core</u> or <u>Mac Mini</u>	Customer Response from <u>Collector</u>
Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)?  Note: Only if your DHCP response is <b>no</b> , enter the following information when prompted:	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.  Recommended: Respond with <b>no</b> :	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.  Recommended: Respond with <b>no</b> :	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.  Recommended: Respond with <b>no</b> :
a. IP address	a. Enter an IP address	a. Enter an IP address	a. Enter an IP address
b. Netmask	b. Enter a netmask using the form 255.255.255.0.	b. Enter a netmask using the form 255.255.255.0.	b. Enter a netmask using the form 255.255.255.0.
c. Enter a gateway IP address for this management (administrative) interface:	c. Enter a gateway IP address.	c. Enter a gateway IP address.	c. Enter a gateway IP address.
d. Enter primary DNS server IP address.	d. Enter the DNS server IP address	d. Enter the DNS server IP address	d. Enter the DNS server IP address
e. Do you have a secondary DNS Server (Yes/No).	e. If <b>yes</b> , enter the IP address of the secondary DNS server.	e. If <b>yes</b> , enter the IP address of the secondary DNS server.	e. If <b>yes</b> , enter the IP address of the secondary DNS server.
f. Do you want to enter the search domains?	f. Enter <b>yes</b> if you want DNS lookups to use a specific domain.	f. Enter <b>yes</b> if you want DNS lookups to use a specific domain.	f. Enter <b>yes</b> if you want DNS lookups to use a specific domain.
g. Enter the search domain (separate multiple search domains by space):	g. Enter space domain(s) separated by spaces; for example: example.com lan.com dom2.com	g. Enter space domain(s) separated by spaces; for example: example.com lan.com dom2.com	g. Enter space domain(s) separated by spaces; for example: example.com lan.com dom2.com
Restart the administrative interface (Yes/No)?	Enter <b>yes</b> to restart with the new configuration settings applied.	Enter <b>yes</b> to restart with the new configuration settings applied.	Enter <b>yes</b> to restart with the new configuration settings applied.

Configuration Wizard Prompts	Customer Response from <a href="#">All-in-One</a>	Customer Response from <a href="#">Core or Mac Mini</a>	Customer Response from <a href="#">Collector</a>
Enter a valid hostname (enter a unique name)	Type a hostname when prompted; do not include the domain; for example: <b>juniperatp1</b>	Type a hostname when prompted; do not include the domain; for example: <b>juniperatp1</b>	Type a hostname when prompted; do not include the domain; for example: <b>juniperatp1</b>
<p>[OPTIONAL] If the system detects a Secondary Core with an eth3 port, then the alternate CnC exhaust option is displayed: Use alternate-exhaust for the analysis engine exhaust traffic (Yes/No)?</p> <p>Enter IP address for the alternate-exhaust (eth2) interface:</p> <p>Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0)</p> <p>Enter gateway IP Address for the alternate-exhaust (eth2) interface: (example:10.6.0.1)</p> <p>Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8)</p> <p>Do you have a secondary DNS server for the alternate-exhaust (eth2) interface?</p> <p>Do you want to enter the search domains for the alternate-exhaust (eth2) interface?</p> <p>Note: A complete network interface restart can take more than 60 seconds</p>	<p>Refer to “Configuring an Alternate Analysis Engine Interface” in the Juniper ATP Appliance Operator’s Guide for more information.</p> <p>Enter yes to configure an alternate eth2 interface.</p> <p>Enter the IP address for the eth2 interface.</p> <p>Enter the eth2 netmask.</p> <p>Enter the gateway IP address.</p> <p>Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface.</p> <p>Enter yes or no to confirm or deny an eth2 secondary DNS server.</p> <p>Enter yes or no to indicate whether you want to enter search domain.</p>	<p>Refer to “Configuring an Alternate Analysis Engine Interface” in the Juniper ATP Appliance Operator’s Guide for more information.</p> <p>Enter yes to configure an alternate eth2 interface.</p> <p>Enter the IP address for the eth2 interface.</p> <p>Enter the eth2 netmask.</p> <p>Enter the gateway IP address.</p> <p>Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface.</p> <p>Enter yes or no to confirm or deny an eth2 secondary DNS server.</p> <p>Enter yes or no to indicate whether you want to enter search domain.</p>	<p>[Traffic Collectors do not send or receive Core analysis engine CnC network traffic, so no eth2 interface is needed.]</p>
Regenerate the SSL self-signed certificate (Yes/No)?	<p>Enter <b>yes</b> to create a new SSL certificate for the Juniper ATP Appliance Server Web UI.</p> <p>If you decline the self-signed certificate by entering <b>no</b>, be prepared to install a certificate authority (CA) certificate.</p>	<p>Enter <b>yes</b> to create a new SSL certificate for the Juniper ATP Appliance Server Web UI.</p> <p>If you decline the self-signed certificate by entering <b>no</b>, be prepared to install a certificate authority (CA) certificate.</p>	Not applicable to Collector.

Configuration Wizard Prompts	Customer Response from <a href="#">All-in-One</a>	Customer Response from <a href="#">Core or Mac Mini</a>	Customer Response from <a href="#">Collector</a>
Enter the following server attributes: Is this a Central Manager device:	Enter Yes; the system will auto-set IP 127.0.0.1 as the All-in-One IP address.	Enter Yes; the system will auto-set IP 127.0.0.1 as the All-in-One IP address.	Enter No; the system will request that you enter the CM IP address now.
Device Name: (must be unique)	Enter the Juniper ATP Appliance Collector Host Name; this identifies the Collector in the Web UI.	Enter a Juniper ATP Appliance Mac Mini or Core/CM Host Name; this identifies the Mac OS X or Core Engine in the Web UI.	Enter the Juniper ATP Appliance Collector Host Name; this identifies the Collector in the Web UI.
Device Description	Enter a device Description	Enter a device Description	Enter a device Description
Device Key PassPhrase  NOTE: Remember this passphrase and use it for all distributed devices!	Enter a user-defined PassPhrase to be used to authenticate the Core to the Central Manager.	Enter the same PassPhrase used to authenticate the Core or Mac Mini to the Central Manager.	Enter the same PassPhrase used to authenticate the Collector to the Central Manager.

### Hardware, Software and Virtual Appliance Access via SSH

To access the Juniper ATP Appliance CLI over the management network:

1. Start a terminal window session and use the **ssh** command to access the appliance.  
For example, if the IP address of the appliance is 10.1.1.2, enter the following command:

```
xssh admin@10.1.1.2
```

2. When prompted, enter your password. By default, the admin user name is **admin** and the password is **1JATP234**.
3. To launch the configuration wizard, enter the command **wizard**.

```
# wizard
```

See [Configuration Wizard Command Prompt Progressions](#) for steps.

### CLI Help and Keyboard Shortcuts

To display Juniper ATP Appliance CLI help, type the command **help** to display CLI keys and auto-completion usage.

For context-sensitive help, alternatively, enter a “?” to display either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference, as described below.

- Enter “?” at the prompt to display a list of the available commands in the current mode.
- Enter “?” after you type a command to display its available options and parameters.
- Enter “?” after a partially typed keyword to display command matches for auto-completions

You can enter commands in abbreviated form if you enter enough characters to uniquely identify each keyword. For example, the show interface command can be abbreviated as:

```
sh in
```

To identify a command's minimum abbreviation, type a few characters then press Tab. When you have entered enough characters, the keyword is completed.

The following table outlines the available CLI shortcuts.

Table 1-1 Keyboard Shortcuts

Action	Shortcut	Description
Auto-Completion	Enter, Tab or Space Key	Completes a partial command during typing if enough characters are typed to uniquely identify it.
Recall	Ctrl+P or ↑	Retrieve previous command from CLI history.
	Ctrl+N or ↓	Retrieve next command from CLI history.
	Ctrl+L or Ctrl+R	Clear the screen or Redisplay the current command line.
Delete	Ctrl+D	Delete character.
	Ctrl+H	Delete character before cursor (Backspace).
	Ctrl+K	Delete all characters from cursor to end of line.
	Ctrl+U or Ctrl+W	Delete all characters or words on line.
Cursor move	Ctrl+A	Move cursor to start of line.
	Ctrl+B	Move cursor back a single character.
	Ctrl+E	Move cursor to end of line.
	Ctrl+F	Move cursor forward a single character.
Character Transpose	Ctrl+T	Transpose character at the cursor with preceding character.
Interrupt output	Ctrl+C	Interrupt presentation of the CLI output.
Replace	!!	Substitute the last command line
	!N	Substitute the Nth command line (absolute as per 'history' command)
	!-N	Substitute the command line entered N lines before (relative)
Exit mode or logout	exit	Exit current mode or exit the CLI session.

### SPECIAL CHARACTER REQUIREMENT

You must enclose non-alphabet characters in double quotes in CLI commands; for example:

```
Juniper ATP Appliance(server)# set passphrase "kfe$nd#$^S"
```

### CLI Modes

The CLI commands that you can enter depend on your user privileges and the CLI command mode. User roles are "admin" and "debugging." The following table describes the CLI command mode.

Note that the prompt in each mode includes the host name of the Juniper ATP Appliance.

Table 1-2 Summary of CLI Modes

Mode	Description	How to Exit
Basic Mode	Monitor system operation and issue basic system commands. This is the default login mode. The following prompt is displayed: JATP#	Enter exit to log out of the CLI.
CM Mode	Monitor system history and upgrades from the Core or vCore in cm (Central Manager) mode. JATP_Hostname# cm JATP_Hostname (cm)# ?	Enter exit to leave cm mode.
Core Configuration Mode	To access Core configuration mode in the Core/CM, All-in-One, and Mac Mini, enter " <b>core</b> " in Basic mode. The prompt changes to indicate the mode in parentheses: JATP_Hostname# core JATP_Hostname (core)# ?	Enter exit to leave server mode.
Collector Configuration Mode	Configure the Juniper ATP Appliance Collector (includes all commands). To access Collector configuration mode, enter " <b>collector</b> " in Basic mode. The prompt changes to indicate the mode in parentheses: JATP_Hostname# collector JATP_Hostname (collector)# ?	Enter exit to leave server mode.
Diagnosis Packet Capture, Monitoring, GSS Reporting and Configuration Mode	Check Initial Setup, Diagnose, Monitor, Set GSS, and Configure the Juniper ATP Appliance (includes all commands). To access Diagnosis mode, enter " <b>diagnosis</b> " in Basic mode. The prompt changes to indicate the mode in parentheses: JATP_Hostname# diagnosis JATP_Hostname (diagnosis)# ?	Enter exit to leave diagnosis mode.
Server Configuration Mode	Set up and monitor the system (includes all Basic commands plus server-specific commands). To access Server configuration mode, enter " <b>server</b> " in Basic mode. The prompt changes to indicate the mode in parentheses: JATP-Hostname# server JATP-Hostname (server)# ?	Enter exit to leave server mode.
Wizard Configuration Mode	Configure the system during installation and setup the management network and connected Juniper ATP Appliance components. To access wizard configuration mode, enter " <b>wizard</b> " in Basic mode. The prompt changes to indicate the mode in parentheses: JATP-Hostname# wizard JATP-Hostname (wizard)# ?	Enter exit to leave wizard mode.



## CHAPTER 2

# All-in-One CLI Commands

This chapter describes the administration commands for a Juniper ATP Appliance All-in-One server appliance, software appliance or virtual appliance.

These commands are used to configure the Juniper ATP Appliance All-in-One appliance, manage configurations, and set system-level settings for interfaces, network services, and SIEM integration.

---

**NOTE** You must enclose non-alphabet characters in double quotes in CLI commands.

---

### Basic Mode Commands

Use general system commands to configure the appliance, view appliance history, enter other CLI modes, obtain help with CLI syntax, and to exit the CLI session.

The general commands are:

- [cm on page 12](#)
- [core on page 13](#)
- [collector on page 12](#)
- [diagnosis on page 14](#)
- [exit on page 14](#)
- [help on page 16](#)
- [history on page 17](#)
- [server on page 20](#)
- [wizard on page 35](#)

Refer to the sections in this guide to review CM Mode, Collector Mode, Core Mode, Diagnosis Mode, Server Mode and Wizard mode commands per device-- All-in-One, CoreCM, Traffic Collector and Mac OS X Detection Engine on a Mac Mini.

## CM Commands

- [exit](#) on page 14
- [help](#) on page 16
- [history](#) on page 17
- [upgrade](#) on page 34

## Core Mode Commands

- [exit](#) on page 14
- [help](#) on page 16
- [history](#) on page 17
- [show \(core mode\)](#) on page 32
- [updateimage](#) on page 35

## Server Mode Commands

- [exit](#) on page 14
- [help](#) on page 16
- [history](#) on page 17
- [ifrestart](#) on page 17
- [ping](#) on page 18
- [reboot](#) on page 18
- [restart](#) on page 19
- [restore](#) on page 20
- [set ip interface \(server mode\)](#) on page 26
- [set system-alert \(server mode\)](#) on page 29
- [set \(server mode\)](#) on page 27
- [shutdown](#) on page 34
- [shutdown](#) on page 34
- [traceroute](#) on page 34

## Collector Mode Commands

- [exit](#) on page 14
- [help](#) on page 16
- [history](#) on page 17
- [set honeypot \(collector mode\)](#) on page 22
- [set traffic-monitoring \(for JATP700 Appliances only\) \(collector mode\)](#) on page 22
- [set traffic-filter \(collector mode\)](#) on page 23
- [set protocols \(collector mode\)](#) on page 23
- [set proxy \(collector mode\)](#) on page 24
- [set traffic-filter \(collector mode\)](#) on page 23
- [show \(collector mode\)](#) on page 31 [show proxy inside or show proxy outside]

## Diagnosis Mode Commands

- [capture-start](#) on page 11
- [copy](#) on page 13
- [exit](#) on page 14
- [gssreport](#) on page 15
- [help](#) on page 16
- [history](#) on page 17
- [set \(diagnosis mode\)](#) on page 25
- [setupcheck](#) on page 30
- [show \(diagnosis mode\)](#) on page 33

## All-in-One CLI Commands

### capture-start

Table 2-1 capture-start

Description	Starts packet capture as a means for diagnosing and debugging network traffic and obtaining stats. See Also: <a href="#">diagnosis</a> [mode]; <a href="#">collector</a> [mode]; <a href="#">copy</a>
Product(s) CLI	<b>All-in-One   Collector</b>
Mode(s)	Diagnosis
Syntax	capture-start
Parameters	<IP address> <interface_name>
Sub-Commands	None
Example	<p>The following example starts a packet capture process on interface eth1 for a Traffic Collector with IP address 8.8.8.8:</p> <pre>hostname # <b>diagnosis</b> hostname (diagnosis) # capture-start 8.8.8.8 eth1</pre> <p><b>NOTE</b> Note: Address 8.8.8.8 need not be a Juniper ATP Appliance. It is just a host that the capture filters on.</p>

**cm**

Table 2-2 cm

Description	Enters cm (Central Manager) mode. See Also: <a href="#">basic</a> [mode];
Product(s) CLI	<b>All-in-One   Core</b>
Mode(s)	Basic
Syntax	cm
Parameters	None
Sub-Commands	exit   help   history   upgrade
Example	The following command example enters cm configuration mode:  hostname # <b>cm</b> hostname (cm) #

**collector**

Table 2-3 collector

Description	Enters the Collector configuration mode. See Also: <a href="#">server</a> [mode]
Product(s) CLI	<b>All-in-One   Collector</b>
Mode(s)	Basic
Syntax	collector
Parameters	None
Sub-Commands	<a href="#">exit</a> ; <a href="#">help</a> ; <a href="#">history</a> ; <a href="#">set (server mode)</a> ; <a href="#">show (collector mode)</a>
Example	The following example enters collector configuration mode:  hostname # <b>collector</b> hostname (collector) # ?

**copy**

Table 2-4 copy

Description	<p>Uses Secure Copy (SCP) to copy and transfer packet capture or traceback (crash) data to a remote location, providing the same authentication and level of security as an SSH transfer.</p> <p>The copy traceback command, upon Customer Support's request, copies the traceback files out of the box to a remote location.</p> <p>See Also: <a href="#">diagnosis [mode]</a>; <a href="#">capture-start</a></p>
Product(s) CLI	<b>All-in-One   Collector   Core-CM   Mac OSX Engine</b>
Mode(s)	Diagnosis
Syntax	<pre>copy capture &lt;scp source_file_name username@destination_host:destination_folder&gt;   traceback {&lt;tab&gt;   ALL} &lt;string URI as user@hostname:path</pre>
Parameters	<pre>copy capture &lt;scp remote filename_location&gt; copy traceback &lt;ALL   filename&gt; copy traceback &lt;tab&gt; [tab displays all available crash filenames]</pre>
Sub-Commands	None
Example	<p>The following example copies the file "Eth1.txt" from the local host to a remote host:</p> <pre>hostname (diagnosis)# copy capture Eth1.txt admin@remotehost.edu:/some/remote/directory</pre>

**core**

Table 2-5 core

Description	<p>Enters core mode.</p> <p>See Also: <a href="#">basic [mode]</a>;</p>
Product(s) CLI	<b>All-in-One   Collector   Core   Mac OS X Detection Engine</b>
Mode(s)	Basic
Syntax	<code>core</code>
Parameters	None
Sub-Commands	<code>exit</code> , <code>help</code> , <code>history</code> , <code>show</code> , <code>updateimage</code>
Example	<p>The following command example enters core configuration mode:</p> <pre>hostname # <b>core</b> hostname (core)#</pre>

**diagnosis**

Table 2-6 diagnosis

Description	Enters the Diagnosis configuration and status check mode. See Also: collector [mode], server [mode]
Product(s) CLI	<b>All-in-One   Collector   Mac OS X Detection Engine</b>
Mode(s)	Basic
Syntax	diagnosis
Parameters	None
Sub-Commands	capture-start; copy; exit; gssreport; help; history; set (server mode); setupcheck; show (diagnosis mode); shutdown
Example	The following example enters diagnosis configuration and status check mode:  hostname # <b>diagnosis</b> hostname (diagnosis) # ?

**exit**

Table 2-7 exit

Description	Ends the CLI session.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Core   Collector   Diagnosis   Server
Syntax	exit
Parameters	None
Example	The following example ends a command mode or CLI session.  <b>JATP# (diagnosis) exit</b> <b>JATP#</b>  <b>JATP (core) exit</b> <b>JATP# exit</b>

**gssreport**

Table 2-8 gssreport

Description	<p>Use the gssreport command to submit reports to Juniper Global Security Services (GSS), and to display the status of the current GSS report.</p> <p>See Also: <a href="#">gssreport</a>; <a href="#">diagnosis</a> [mode]</p>
Product(s) CLI	<b>All-in-One   Collector   Mac OS X Detection Engine</b>
Mode(s)	diagnosis
Syntax	<code>gssreport status   submit</code>
Parameters	<p><code>status</code> - displays the status of the current GSS report.</p> <p><code>submit</code> - submits a report to Juniper ATP Appliance GSS.</p>
Sub-Commands	None
Example	<p>The following examples display the status of a GSS report submission:</p> <pre>hostname # <b>diagnosis</b> hostname (diagnosis)# gssreport submit Successfully started GSS report  hostname (diagnosis)# gssreport status GSS is currently enabled Last 5-minute GSS report at 2015-07-28 10:34:24.414322: successfully submitted Last hourly GSS report at 2015-07-28 10:34:24.468259: successfully submitted Last daily GSS report at 2015-07-28 10:34:28.225512: successfully submitted</pre>

## help

Table 2-9 help

Description	Displays information about the CLI help system.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Core   Collector   Diagnosis   Server
Syntax	help
Parameters	None
Example	<p>The following example shows some of the output of the help command.</p> <pre>CONTEXT SENSITIVE HELP [?] - Display context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference.  AUTO-COMPLETION The following keys both perform auto-completion for the current command line. If the command prefix is not unique then the bell will ring and a subsequent repeat of the key will display possible completions.  [enter] - Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending part of the command line will be highlighted and explained. [tab]   - Auto-completes [space] - Auto-completes, or if the command is already resolved inserts a space.  If "&lt;cr&gt;" is shown, that means that what you have entered so far is a complete command, and you may press Enter (carriage return) to execute it.  Use ? to learn command parameters and option:  <b>JATP (server)#</b> show f? firewall Show the firewall configuration settings         interface <b>JATP (server)#</b> show firewall? all      Show the current iptables settings whitelist Show the iptables whitelist settings show firewall whitelist? &lt;cr&gt; show firewall whitelist</pre>



**history**

Table 2-10 history

Description	Displays the current CLI session command line history.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Core   Collector   Diagnosis   Server
Syntax	<code>history</code>
Parameters	None
Example	The following examples returns command line history for the current CLI session. <b>JATP# (core) history</b>

**ifrestart**

Table 2-11 ifrestart

Description	Restarts the interface driver and services using the interface.
Product(s) CLI	<b>All-in-One   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server
Syntax	<code>ifrestart eth0 eth1</code>
Parameters	<div>eth0 Restarts the management network administra interface.</div> <div>eth1 Restarts the monitoring network interface.</div>
Example	The following example restarts the <code>eth0</code> interface for the management network. <code>&lt;FireEye_name&gt;# ifrestart eth0</code>

## ping

Table 2-12 ping

Description	Sends ICMP (Internet Control Message Protocol) echo request packets to a specified host name or IP address to verify that the destination is reachable over the network.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	<b>ping</b> [-c <i>count</i> ] [-h <i>hops</i> ] [ <i>string</i> ]	
Parameters	<div>-c <i>count</i></div> <div>-h <i>hops</i></div> <div><i>string</i></div>	<div>Number of echo requests to send. By default, pings are continuously until you press Ctrl+C.</div> <div>Number of next hops between pings (default is 1).</div> <div>IP address, hostname or interface name used to ping device address.</div>
Example	<p>The following example sends three echo requests to the device with the IP Address 10.10.10.1</p> <pre>&lt;FireEye_name&gt;# ping -c 3 10.10.10.1 PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data. 64 bytes from 10.10.10.1: icmp_req=1 ttl=64 time=0.314 ms 64 bytes from 10.10.10.1: icmp_req=2 ttl=64 time=0.277 ms 64 bytes from v: icmp_req=3 ttl=64 time=0.274 ms  --- 10.10.10.1 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 1999ms rtt min/avg/max/mdev = 0.274/0.288/0.314/0.022 ms</pre>	

## reboot

Table 2-13 reboot

Description	Reboots the Juniper ATP Appliance.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	<b>reboot</b>	
Parameters	None	
Example	<p>The following example reboots the system.</p> <pre>hostname# <b>reboot</b></pre>	

**restart**

Table 2-14 restart

Description	Restarts Juniper ATP Appliance services.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	restart [all   behaviorengine   cm   collector   core   correlationengine   database   ntpserver   sshserver   staticengine   webserver]	
Parameters	all behaviorengine cm collector core correlationengine database ntpserver sshserver staticengine webserver	Restarts all Juniper ATP Appliance services. Restarts the Behavioral Analysis Engine. Restarts the Central Manager Web UI service. Restarts the Collector service. Restarts the Core Detection Engine. Restarts the Correlation Engine. Restarts the Database. Restarts the NTP server. Restarts the SSH server. Restarts the Static Analysis Engine. Restarts the web server.
Example	The following example restarts the Central manager service. <b>JATP# restart cm</b>	

## restore

Table 2-15 restore

Description	Restores the system configuration to the factory default settings. This will only reset the password to default temporarily.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	<pre>restore [support   firewall {backup   default}   hostname   network]</pre> <p>Whitelist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the whitelist state as rules cannot be saved in that case.</p>	
Parameters	<div>support</div> <div>firewall {backup   default}</div> <div>hostname</div> <div>network</div>	<div>Restores the default support password setting remote login (set during initial installation per l See also (server)# <a href="#">set (server mode) support</a></div> <div>Restores the firewall settings from either the p backup, or from the default factory settings.</div> <div>Restores the system's hostname to the factory hostname.</div> <div>Restores the IP address and DNS settings to th factory default settings.</div> <div>WARNING: This command option removes the IP address and DNS settings, and reloads the d values for these settings.</div>
Example	<p>The following example restores the system.</p> <pre>JATP# <b>restore</b></pre> <p>This next example restores the SSH login "support" password to the default.</p> <pre>JATP # restore support password</pre> <p>Restore the default support password? (Yes/No)? yes</p> <p>support password was restored successfully!</p>	

## server

Table 2-16 server

Description	Enters the server configuration mode. See Also: <a href="#">collector</a>
Product(s) CLI	<b>All-in-One   Collector   Core/CM   Mac Mini Mac OS X</b>
Mode(s)	Basic
Syntax	<code>server</code>
Sub-Commands	<a href="#">exit</a> ; <a href="#">help</a> ; <a href="#">history</a> ; <a href="#">ifrestart</a> ; <a href="#">ping</a> ; <a href="#">reboot</a> ; <a href="#">restore</a> ; <a href="#">set (server mode)</a> ; <a href="#">upgrade</a> Whitelist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the whitelist state as rules cannot be saved in that case.

Table 2-16 server

Example	<p>The following example enters server configuration mode:</p> <pre>hostname # <b>server</b> hostname (server) # ?</pre>
---------	--

**set honeypot (collector mode)**

Table 2-17 set honeypot

Description	<p>Enables and disables the SSH-Honeypot feature for a Traffic Collector.</p> <p>A honeypot can be deployed within a customer network to detect network activity generated by malware attempting to infect or attack other machines in a local area network. These attempted SSH logins can be used to supplement detection of lateral spread.</p> <p>There are two parameters that can be set for a honeypot:</p> <ul style="list-style-type: none"> <li>• Enable/disable a honeypot</li> <li>• Set a Static IP (IP, mask, and gateway) or DHCP of a publicly addressable interface</li> </ul> <p>See Also: show honeypot command in <a href="#">show (collector mode)</a></p>
Product(s) CLI	<b>All-in-One   Collector</b>
Mode(s)	collector
Syntax	<pre>(collector)# set honeypot ssh-honeypot enable dhcp (collector)# set honeypot ssh-honeypot enable address (IP address) netmask (subnet IP) gateway (IP address) (collector):# set honeypot ssh-honeypot disable</pre>
Example	<p>The following example enables the SMB parser for lateral detections:</p> <pre>(collector)# set honeypot ssh-honeypot enable address 1.2.3.4 netmask 255.255.0.0 gateway 1.2.3.1</pre> <p><b>NOTE</b> The static IP configuration does not require configuring DNS. Honeypots do not require a DNS server at this time.</p>

**set traffic-monitoring (for JATP700 Appliances only) (collector mode)**

Table 2-18 set traffic-monitoring

Description	Sets the traffic monitoring interface on the JATP700
Product(s) CLI	<b>All-in-One   Collector</b>
Mode(s)	collector
Syntax	<pre># set traffic-monitoring-ifc 1gb_ifc</pre> <p>Set the traffic monitoring interface to be the 1G interface.</p> <pre># set traffic-monitoring-ifc 10gb_ifc</pre> <p>Set the traffic monitoring interface to be the 10G interface.</p> <p><b>NOTE</b> After making an interface type change, the system must be rebooted for the change to take effect.</p>

**set traffic-filter (collector mode)**

Table 2-19 set traffic-filter

Description	<p>Sets traffic filter rules to avoid analysis on a set of configured traffic, which cannot be made retroactive; for example: any analysis skipped as a result of the filtering cannot be reversed. This command can be applied to an entire network/subnet/CIDR range.</p> <p>See Also: <a href="#">set (server mode)</a>; show (diagnosis mode) [<a href="#">show traffic-filter</a>]</p>		
Product(s) CLI	<b>All-in-One   Collector</b>		
Mode(s)	collector		
Syntax	<pre>set traffic-filter {add &lt;rule_name&gt; &lt;domain&gt; &lt;source-address&gt; &lt;destination-address&gt; &lt;source-port&gt; &lt;destination-port&gt; &lt;protocol&gt;   remove &lt;rule_name&gt;}</pre>		
Parameters	<table border="0"> <tr> <td style="vertical-align: top;"> <pre>traffic-filter add &lt;RuleString&gt;&lt;DomainString&gt;&lt;source-address&gt;&lt;destination-address&gt; &lt;source-port&gt; &lt;destination-port&gt; &lt;protocol&gt;</pre> </td><td style="vertical-align: top;"> <p>Adds a traffic filter rule where:</p> <p>“RuleString” is the name of the rule</p> <p>“DomainString” is the domain to filter out</p> <p>“source-address” is the source IPv4 address or network (CIDR)</p> <p>“destination-address” is the destination IPv4 address or network (CIDR)</p> <p>“source-port” is the source port number (0-65535)</p> <p>“destination-port” is the destination port number (0-65535)</p> <p>“protocol” is the protocol type: either IP, TCP, UDP or HTTP</p> </td></tr> </table>	<pre>traffic-filter add &lt;RuleString&gt;&lt;DomainString&gt;&lt;source-address&gt;&lt;destination-address&gt; &lt;source-port&gt; &lt;destination-port&gt; &lt;protocol&gt;</pre>	<p>Adds a traffic filter rule where:</p> <p>“RuleString” is the name of the rule</p> <p>“DomainString” is the domain to filter out</p> <p>“source-address” is the source IPv4 address or network (CIDR)</p> <p>“destination-address” is the destination IPv4 address or network (CIDR)</p> <p>“source-port” is the source port number (0-65535)</p> <p>“destination-port” is the destination port number (0-65535)</p> <p>“protocol” is the protocol type: either IP, TCP, UDP or HTTP</p>
<pre>traffic-filter add &lt;RuleString&gt;&lt;DomainString&gt;&lt;source-address&gt;&lt;destination-address&gt; &lt;source-port&gt; &lt;destination-port&gt; &lt;protocol&gt;</pre>	<p>Adds a traffic filter rule where:</p> <p>“RuleString” is the name of the rule</p> <p>“DomainString” is the domain to filter out</p> <p>“source-address” is the source IPv4 address or network (CIDR)</p> <p>“destination-address” is the destination IPv4 address or network (CIDR)</p> <p>“source-port” is the source port number (0-65535)</p> <p>“destination-port” is the destination port number (0-65535)</p> <p>“protocol” is the protocol type: either IP, TCP, UDP or HTTP</p>		
Example	<p>The following example add a traffic filter rule to the Traffic Collector.</p> <pre>JATP-collector02(collector)# set traffic-rule add CustomRule2 headqrts.example.com 10.2.0.0/16 20.0.0.2 90 120 tcp</pre> <p>where destination-address is 20.0.0.2, destination-port is 120, protocol is tcp, source-address is 10.2.0.0/16 and source-port is 90 (in our example).</p>		

**set protocols (collector mode)**

Table 2-20 set protocols

Description	<p>Enables and disables the HTTP or SMB parser for a Traffic Collector.</p> <p>See Also: <a href="#">show protocols</a> command in <a href="#">show (collector mode)</a></p>
Product(s) CLI	<b>All-in-One   Collector</b>
Mode(s)	collector
Syntax	<pre>(collector)# set protocols {http [on off]   smb [on off]}</pre>
Example	<p>The following example enables the SMB parser for lateral detections:</p> <pre>hostname (collector) set protocols smb on</pre>

**set proxy (collector mode)**

Table 2-21 set proxy

Description	<p>Sets an Inside or Outside data path proxy from collector mode.</p> <p>Deploy Traffic Collectors in locations where the monitoring interface is (1) placed “outside” between the proxy and the egress network for customer environments in which the proxy supports XFF (X-Forwarded-For), or (2) [the more typical deployment scenario], the Collector is placed between the proxy and the internal network using FQDN (if available) to identify the threat source for all types of incidents (“inside” proxy). When configured, the Juniper ATP Appliance Traffic Collector will monitor all traffic and correctly identify source and destination hosts for each link in the kill chain wherever the data allows for it.</p> <p>Note that if the “X-Forwarded-For” header is provided in the HTTP request, detection will identify threat targets when deployed outside of the proxy (customers can choose to disable the XFF feature in the proxy setting, if desired).</p> <p>See Also: <a href="#">set (server mode)</a> [“set proxy” command for management network]; <a href="#">set (diagnosis mode)</a>;</p> <p><b>NOTE</b> The mitigation IP address of a CNC server is not be available for Inside proxy deployments. When a Juniper ATP Appliance is deployed behind a proxy, the Mitigation-&gt; Firewall page in the Juniper ATP Appliance Central Manager Web UI (which typically displays the CNC server IP address to mitigate) will be empty. The destination IP address of any callback is made to the proxy server ip address, so it is not relevant to display the proxy server IP address on the Mitigation-&gt;Firewall page.</p>	
Product(s) CLI	<b>All-in-One   Collector</b>	
Mode(s)	collector	
Syntax	<pre>set proxy inside {add &lt;proxy IP address&gt; &lt;proxy port&gt;   remove &lt;proxy IP address&gt; &lt;proxy port&gt;}  set proxy outside {add &lt;proxy IP address&gt;   remove &lt;proxy IP address&gt;}</pre>	
Parameters	<div>inside</div> <div>outside</div> <div>add</div> <div>remove</div>	<div>Sets the inside proxy IP addresses</div> <div>Sets the outside proxy IP addresses</div> <div>Adds a proxy configuration.</div> <div>Removes a proxy configuration.</div>
Example	<p>The following example sets an inside data path proxy:</p> <pre>JATP (collector)# set proxy inside add 10.1.1.1 8080</pre> <p>The following example sets an outside data path proxy:</p> <pre>JATP (collector)# set proxy outside add 10.2.1.1</pre>	



**set (diagnosis mode)**

Table 2-22 set

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also: <a href="#">set (server mode)</a> ; set (collector mode)	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	diagnosis	
Syntax	set logging	
Parameters	all	Sets logging for all Juniper ATP Appliance components.
	default	Sets logging to the default parameters
	debug	Sets logging at the debug level.
	info	Sets logging at the info level.
	warning	Sets logging at the warning level.
	error	Sets logging at the error level.
	critical	Sets logging at the critical level.
Example	<p>The following example sets the default logging level for all Juniper ATP Appliance components.</p> <pre>JATP# set logging all</pre>	

## set ip interface (server mode)

Table 2-23 set ip interface

Description	<p>Sets the management interface (eth0) and/or the alternate-exhaust interface (eth2) for the Juniper ATP Appliance.</p> <p>Refer to the Operator's Guide for information about configuring the optional alternate analysis engine eth2 interface option (it moves CnC traffic during analysis engine processing off the enterprise's eth0 management network).</p> <p>See Also: <a href="#">set (server mode)</a>; <a href="#">set protocols (collector mode)</a>; <a href="#">show (core mode)</a>; <a href="#">shutdown</a></p>	
Product(s) CLI	<b>All-in-One   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	server	
Syntax	<pre>(server) # set ip interface management &lt;dhcp   address   netmask   gateway&gt;  (server) # set ip interface alternate-exhaust &lt;address   netmask   gateway&gt;</pre>	
Parameters	<div>dhcp</div> <div>address</div> <div>netmask</div> <div>gateway</div>	<div>Enables DHCP for the management or alternate-exhaust interface.</div> <div>Sets the static IP address for the management (eth0) or alternate-exhaust (eth2) interface,</div> <div>Sets the netmask for the management network or the alternate-exhaust network.</div> <div>Sets the Gateway IP address for the management interface or the optional alternate-exhaust network.</div>
Example	<p>The following example configures the management interface (eth0) for a Juniper ATP Appliance Core device:</p> <pre>JATP (server)# set ip interface management address 10.2.123.18 netmask 255.255.255.0 gateway 10.2.0.1</pre> <p>The following example configures the management interface (eth0) using DHCP:</p> <pre>JATP (server)# set ip interface management dhcp</pre> <p>This example configures the alternate-exhaust interface (eth2) for a Juniper ATP Appliance Core device:</p> <pre>JATP (server)# set ip interface alternate-exhaust address 10.2.123.12 netmask 255.255.255.0 gateway 10.2.0.2</pre>	

**set (server mode)**

Table 2-24 set

Description	Configure the system settings.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server, See Also: <a href="#">set (diagnosis mode)</a> ; <a href="#">set traffic-filter (collector mode)</a>
Syntax	<pre>set [autoupdate {on   off}   cli timeout secs   clock   cm address   support {enable   disable} localmode {enable   disable}  passphrase <i>string</i>   dns   firewall {all &lt;backup   flush&gt;   whitelist}   hostname <i>string</i>   ip interface {management   alternate-exhaust}  ntpserver   password   proxy {config   enabled   remove}   timezone <i>string</i>   uipassword]</pre>
Parameters (Columns below)	<p>Note: vCore for AWS does not use the following CLI commands:  set ip  set hostname</p> <p>[Users cannot set static IP address or change the hostname directly on an EC2 AWS instance]</p> <p>server mode “set proxy” command is a management network proxy tool; for data path Collector proxy configurations, refer to <a href="#">set proxy (collector mode)</a>.</p>
autoupdate {content   software} {on   off}	Turn on or off automatic product updates. <pre>set autoupdate content on</pre>
cli timeout <i>secs</i>	Sets CLI timeout period in seconds (0 indicates no timeout).
clock	Sets the current date and time.
cm <i>address</i>	Sets the IP address of the Central Manager and netmask using the slash notation; example: AAA.BBB.CCC.DD/X
set support {enable   disable}   {localmode}	Enables remote SSH login “support” account or localmode enable/disable.
dns	Sets DNS (or enables DHCP for DNS) for the management interface by default if interface is unspecified.
firewall {all <backup   flush>   whitelist <add   delete   flush>}	<p>Backs up or flushes (clears) all current iptables for a firewall, or adds, deletes or flushes the current iptables whitelist-specific settings for the firewall.</p> <p>The “add” option adds an IP address to the iptables outbound whitelist.</p> <pre># set firewall whitelist add 10.1.1.1</pre>

Table 2-24 `set`

<code>hostname string</code>	Sets the system's host name.
<code>ip interface {management   alternate-exhaust} &lt;dhcp   address   netmask   gateway&gt;</code>	Sets the IP address, netmask, or default gateway, or enables DHCP for the management or alternate-exhaust interface.
<code>ntpserver</code>	Sets the Network Time Protocol (NTP) server.
<code>passphrase string</code>	Sets the device key password; enter a string.
<code>password</code>	Sets a new password for the CLI administrator.
<code>proxy {config &lt;all http&gt;   enabled &lt;on off&gt;   remove &lt;all http&gt;}</code>	Config, enable/disable, or remove “all” proxy configs, or remove an HTTP-specific proxy server.  <div> <b>TIP</b> Tip: Config the proxy for “all” protocols first, and then change HTTP proxy as needed. </div>
<code>timezone string</code>	Sets the timezone for the device.
<code>uipassword</code>	Sets a new admin password for CM Web UI access.
Example	<p>The following example disables the CLI timeout counter.</p> <pre>JATP (server) # set cli timeout 0</pre> <p>The following example enables support:</p> <pre>JATP (server) # set support enable</pre>

**set system-alert (server mode)**

Table 2-25 set system-alert

Description	<p>Configure the traffic threshold and checking interval for the Collector “monitored traffic” health status.</p> <p>When the monitored traffic of a collector within the checking interval time is lower than the threshold, a system health alert is generated. You can send an email notification of the alert if email notifications of system health events are configured.</p>
Product(s) CLI	<b>All-in-One   Core CM</b>
Mode(s)	Server, See Also: <a href="#">set (diagnosis mode)</a> ; <a href="#">set traffic-filter (collector mode)</a> ; <a href="#">show</a>
Syntax	<pre>set system-alert traffic &lt;integer&gt; time &lt;interval&gt;</pre> <p><b>NOTE</b> Note that both "traffic" and "time" parameters are required in order to set the threshold for both the minimum traffic and time.</p>
Parameters	<p><b>traffic</b> - the minimum traffic (in KB)</p> <p><b>interval</b> - the checking interval (in minutes)</p>
Example	<pre>JATP (server) # set system-alert traffic 100 time 30</pre> <p>This example sets the system alert such that, if the total monitored traffic of a collector within the last 30 minutes dips lower than 100KB, then a system health alert will be generated (and users will receive an email notification of the alert if email notifications are configured for system health events).</p> <p>By default this alert is disabled, and users must set the minimum traffic and interval in order to enable it. Also note that all bytes seen on Ethernet frames are counted in the traffic.</p> <p>The minimum interval for the "set system-alert traffic" time interval command is 10 minutes. If the minimum interval is set to less than 10 minutes, no alerts will be triggered.</p>

## setupcheck

Table 2-26 setupcheck

Description	Checks and reports on basic configuration settings and analysis pipeline setup.	
Product(s) CLI	<b>All-in-One   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	diagnosis	
Syntax	setupcheck {all   report   basic   analysis}	
Parameters	all	Checks both basic settings and analysis pipeline.
	report	Shows report of last setupcheck.
	basic	Checks basic configuration settings.
	analysis	Checks the analysis pipeline.
Example	<p>The following example checks all basic configuration settings as well as the analysis pipeline:</p> <pre>JATP (diagnosis) # setupcheck all</pre>	

**show (collector mode)**

Table 2-27 show (collector mode)

Description	Displays the Traffic Collector HOMENET settings and all configured subnets, as well as current traffic filters and the current XFF status (enabled or disabled)								
Product(s) CLI	<b>All-in-One   Collector</b>								
Mode(s)	Collector								
Subcommands	homenet   traffic-filter   proxy   honeypot								
Syntax	show								
Parameters	<table> <tr> <td>traffic-filter</td><td>Shows all traffic filter rules.</td></tr> <tr> <td>protocols</td><td>Shows current HTTP or SMB protocol parser settings</td></tr> <tr> <td>proxy {inside   outside}</td><td>Shows Traffic Collector proxy for inside or outside configurations.</td></tr> <tr> <td>honeypot</td><td>Shows the current honeypot configuration.</td></tr> </table>	traffic-filter	Shows all traffic filter rules.	protocols	Shows current HTTP or SMB protocol parser settings	proxy {inside   outside}	Shows Traffic Collector proxy for inside or outside configurations.	honeypot	Shows the current honeypot configuration.
traffic-filter	Shows all traffic filter rules.								
protocols	Shows current HTTP or SMB protocol parser settings								
proxy {inside   outside}	Shows Traffic Collector proxy for inside or outside configurations.								
honeypot	Shows the current honeypot configuration.								
Example	<p>The following example displays the current Collector proxy inside settings:</p> <pre>collector02 (collector) # show proxy inside Proxy IPs: 10.1.1.1</pre> <p>The following example displays the current traffic filter:</p> <pre>collector02 (collector) # show traffic-filter Name: CustomRule2, Domain: headqtrs.example.com</pre> <p>The following example displays the current SMB protocol parser setting:</p> <pre>collector02 (collector) # show protocols</pre> <p>The following example displays the current honeypot configuration:</p> <pre>collector02 (collector) # show honeypot ssh-honeypot</pre>								

**show (collector mode)**

Table 2-28 show (collector mode)

Description	Display the currently selected traffic monitoring interface.
Product(s) CLI	<b>All-in-One   Collector</b>
Mode(s)	Collector
Syntax	<pre>collector02 (collector) # ow traffic-monitoring-ifc-type</pre> <p>Display the currently selected traffic monitoring interface</p>

**show (core mode)****Table 2-1**

Description	Displays the guest image(s) status or whitelist statistics. See Also: <a href="#">shutdown</a> ; <a href="#">show (diagnostic mode)</a>	
Product(s) CLI	<b>All-in-One   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Core	
Syntax	show	
Parameters	images	Displays guest image update and status information.
	whitelist	Displays the name, hit count and the time of last hit of a user configured whitelist.  Note that when a whitelist rule is deleted, it will be removed from the list. Updates to existing rule are not affected by the presence of the rule in the output, but hit count could increment. Further, more than one rule can be hit by a single incident.
	alternate-exhaust-interface	Displays the status of the alternate exhaust interface eth2.
Example	The following example demonstrates the show images command usage:  JATP(core)# show images	
	The following example demonstrates the show whitelist command usage:  JATP(core)# show whitelist  JATP(core)# show whitelist Rule Name    Hit Count    Local Time of Last Hit URI1            10            Wed Sep 2 18:16:55 2015 URI2            10            Wed Sep 2 18:16:55 2015 URI3            10            Wed Sep 2 18:16:55 2015 greatfilesarey 49            Wed Sep 2 18:20:00 2015	
	The following example shows how to get the alternate-exhaust interface (eth2) status:  JATP(core)# show alternate-exhaust interface	



**show (diagnosis mode)**

Table 2-29 show

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also: <a href="#">shutdown</a> ; <a href="#">show (core mode)</a>	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	diagnosis	
Syntax	show	
Parameters	<div>device {collectorstatus     corestatus   slavecorestatus}</div> <div>protocol {web   email}</div> <div>objects</div> <div>logging</div> <div>log error traceback</div> <div>log error last &lt;integer: number of lines to display&gt;</div>	<div>Display connected device statistics for Traffic Collector, CoreCM, or Mac Mini Detection Engine Secondary "slave core."</div> <div>Displays the session counts for network web or email protocols.</div> <div>Displays the current number of file objects.</div> <div>Displays the currently-configured logging level. See Also: <a href="#">set traffic-filter (collector mode) logging</a></div> <div>Displays only the tracebacks (if any) generated by Juniper ATP Appliance OS process error logs. A traceback is a stack of functions that were executing when an error condition was encountered.</div> <div>Displays n [1-1000] lines of the contents of the common log file.  Example: show log error last 12</div>
Example	<p>The following example displays the connected Traffic Collector status.</p> <pre>JATP(diagnosis)# show device collectorstatus &lt;cr&gt;  JATP (diagnosis)# show device collectorstatus WEB_COLLECTOR ===== ==== IP : 10.2.9.68 Enabled : True Last Seen : 2015-07-25 15:13:17.967000-07:00 Install Date : 2015-06-25 19:03:38-07:00 ===== ==== IP : 10.2.20.3 Enabled : True Last Seen : 2015-07-28 11:07:42.046000-07:00 Install Date : 2013-11-14 09:25:39-08:00</pre> <p>This example displays the log error traceback</p> <pre>JATP(diagnosis)# show log error traceback &lt;cr&gt;</pre>	

**shutdown**

Table 2-30 shutdown

Description	Shuts down the Juniper ATP Appliance server.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server
Syntax	shutdown
Parameters	None
Example	The following example performs a shutdown of the current device. JATP# <b>shutdown</b>

**traceroute**

Table 2-31 traceroute

Description	Displays the route packets trace to a host name or an IP address.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server   Collector
Syntax	traceroute
Parameters	<div> <div>-h unsigned integer</div> <div>Specifies the number of hops</div> </div> <div> <div>string</div> <div>Names the remote system to be traced.</div> </div>
Example	The following example performs a traceroute of the named device. JATP# <b>traceroute -h 2 MacMininOSX-Engine</b>

**upgrade**

Table 2-32 upgrade

Description	Upgrade Juniper ATP Appliance software for the Core/CM device or vCore, and all connected physical or virtual devices.
Product(s) CLI	<b>All-in-One   Core CM</b>
Mode(s)	cm
Syntax	upgrade <URI as user@hostname:path>
Parameters	<div> <div>&lt;String_URI&gt;</div> <div>Specifies the software packages to copy .from a remote location for upgrading via the Core.</div> </div>
Example	The following example copies Juniper ATP Appliance software to the Core from a remote location defined by the path provided. <b>CoreCM(cm) # upgrade admin@remoteHost.edu:some/remote/directory</b>

**updateimage**

Table 2-33 updateimage

Description	Update or correct the guest-image OS profile used by the detection and analysis behavioral engine. The updateimage command will update the guest images from the Juniper ATP Appliance update servers or a USB drive attached to the Juniper ATP Appliance.
Product(s) CLI	<b>All-in-One   Core-CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Core
Syntax	updateimage
Parameters	<code>built-in</code> Updates the guest-image on the detection Engine.
Example	The following example performs a built-in profile update for the Core detection engine.  <pre> JATP (core)# updateimage built-in Installing image SC-XP-20150617.img... Previous version of SC-XP-20150617.img exists. Checking integrity... Image SC-XP-20150617.img is already installed Installing image SC-W7-20150521.img... Previous version of SC-W7-20150521.img exists. Checking integrity... Image SC-W7-20150521.img is already installed </pre>

**wizard**

Table 2-34 wizard

Description	Enters the Configuration Wizard. For Configuration Wizard commands and response, see “Configuration Wizard for the All-in-One Server” in the next section to follow command prompts and recommended responses.
Product(s) CLI	<b>All-in-One   Core/CM   Collector   Mac Mini Mac OS X</b>
Mode(s)	Basic
Syntax	wizard
Parameters	None
Example	The following command starts the configuration wizard.  <pre> hostname # wizard </pre>

## Configuration Wizard for the All-in-One Server

Table 2-35 Configuration Wizard for All-in-One Server

Configuration Wizard Prompts	Customer Response Actions
<p>Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)?</p> <p>Note: Only if your DHCP response is <b>no</b>, enter the following information when prompted:</p> <ul style="list-style-type: none"> <li>a. IP address (no CIDR format)</li> <li>b. Netmask</li> <li>c. Enter a gateway IP address for this management (administrative) interface:</li> <li>d. Enter primary DNS server IP address.</li> <li>e. Do you have a secondary DNS Server (Yes/No).</li> <li>f. Do you want to enter the search domains?</li> <li>g. Enter the search domain (separate multiple search domains by space):</li> </ul> <p>Restart the administrative interface (Yes/No)?</p>	<p>We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.</p> <p>Recommended: Respond with <b>no</b>:</p> <ul style="list-style-type: none"> <li>a. Enter an IP address</li> <li>b. Enter a netmask using the form 255.255.255.0.</li> <li>c. Enter a gateway IP address.</li> <li>d. Enter the DNS server IP address</li> <li>e. If <b>yes</b> enter the IP address of the secondary DNS server.</li> <li>f. Enter <b>yes</b> if you want DNS lookups to use a specific domain.</li> <li>g. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com</li> </ul> <p>Enter <b>yes</b> to restart with the new configuration settings applied.</p>
Enter a valid hostname.	Type a hostname when prompted; do not include the domain; for example: <b>JuniperATP1</b>
<p>[OPTIONAL]</p> <p>If the system detects a Secondary Core with an eth2 port, then the alternate CnC exhaust option is displayed:</p> <p>Use alternate-exhaust for the analysis engine exhaust traffic (Yes/No)?</p> <p>Enter IP address for the alternate-exhaust (eth2) interface:</p> <p>Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0)</p> <p>Enter gateway IP Address for the alternate-exhaust (eth2) interface: (example:10.6.0.1)</p> <p>Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8)</p> <p>Do you have a secondary DNS server for the alternate-exhaust (eth2) interface?</p> <p>Do you want to enter the search domains for the alternate-exhaust (eth2) interface?</p> <p>Note: A complete network interface restart can take more than 60 seconds</p>	<p>Refer to “Configuring an Alternate Analysis Engine Interface” in the Juniper ATP Appliance Operator’s Guide for more information.</p> <p>Enter <b>yes</b> to configure an alternate eth2 interface.</p> <p>Enter the IP address for the eth2 interface.</p> <p>Enter the eth2 netmask.</p> <p>Enter the gateway IP address.</p> <p>Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface.</p> <p>Enter <b>yes</b> or <b>no</b> to confirm or deny an eth2 secondary DNS server.</p> <p>Enter <b>yes</b> or <b>no</b> to indicate whether you want to enter search domain.</p>
Regenerate the SSL self-signed certificate (Yes/No)?	Enter <b>yes</b> to create a new SSL certificate for the Juniper ATP Appliance Server Web UI.

## CHAPTER 3

# Core/CM Server CLI Commands

This chapter describes the commands available for Juniper ATP Appliance Core/CM or vCore servers. These commands are used to configure devices and software, manage security events, and show system information and status.

You must enclose non-alphabet characters in double quotes in CLI commands.

### Basic Mode Commands

Use general system commands to configure the appliance, view appliance history, enter other CLI modes, obtain help with CLI syntax, and to exit the CLI session.

The general commands are:

- [cm on page 39](#)
- [core on page 40](#)
- [diagnosis on page 41](#)
- [exit on page 42](#)
- [help on page 43](#)
- [history on page 44](#)
- [server on page 48](#)
- [wizard on page 59](#)

Refer to the respective sections in this guide to review Diagnosis Mode, CM Mode, Collector Mode and Server Mode commands per product device.

### CM Commands

- [exit on page 42](#)
- [help on page 43](#)
- [history on page 44](#)
- [upgrade on page 58](#)

## Core Mode Commands

- [exit](#) on page 42
- [help](#) on page 43
- [history](#) on page 44
- [set \(core mode\)](#) on page 48
- [show \(core mode\)](#) on page 53
- [updateimage](#) on page 59

## Server Mode Commands

- [exit](#) on page 42
- [help](#) on page 43
- [history](#) on page 44
- [ifrestart](#) on page 44
- [ping](#) on page 45
- [reboot](#) on page 45
- [restart](#) on page 45
- [restore](#) on page 47
- [set \(server mode\)](#) on page 50
- [server](#) on page 48
- [show \(server mode\)](#) on page 55
- [shutdown](#) on page 58
- [traceroute](#) on page 58
- [upgrade](#) on page 58

## Diagnosis Mode Commands

- [capture-start](#) on page 39
- [copy](#) on page 41
- [exit](#) on page 42
- [gssreport](#) on page 42
- [help](#) on page 43
- [history](#) on page 44
- [set \(diagnosis mode\)](#) on page 52
- [setupcheck](#) on page 52
- [show \(diagnosis mode\)](#) on page 54

## CoreCM CLI Commands

### capture-start

Table 3-1 capture-start

Description	Starts packet capture as a means for diagnosing and debugging network traffic and obtaining stats (not part of the Collector traffic capture engine).  See Also: <a href="#">diagnosis</a> [mode]; <a href="#">copy</a>
Product(s) CLI	<b>All-in-One   Collector   Core   Mac OS X Detection Engine</b>
Mode(s)	Diagnosis
Syntax	capture-start
Parameters	<IP address> <interface_name>
Sub-Commands	None
Example	<p>The following example starts a packet capture process on interface eth1 for a Juniper ATP Appliance with IP address 8.8.8.8:</p> <pre>hostname # <b>diagnosis</b> hostname (diagnosis)# capture-start 8.8.8.8 eth1</pre> <p><b>NOTE</b> Address 8.8.8.8 need not be a Juniper ATP Appliance. It is just a host that the capture filters on.</p>

### cm

Table 3-2 cm

Description	Enters cm (Central Manager) mode.  See Also: <a href="#">basic</a> [mode];
Product(s) CLI	<b>All-in-One   Core</b>
Mode(s)	Basic
Syntax	cm
Parameters	None
Sub-Commands	exit   help   history   upgrade
Example	<p>The following command example enters cm configuration mode:</p> <pre>hostname # <b>cm</b> hostname (cm) #</pre>

**core**

Table 3-3 core

Description	Enters core mode.  See Also: <a href="#">basic</a> [mode];
Product(s) CLI	<b>All-in-One   Collector   Core   Mac OS X Detection Engine</b>
Mode(s)	Basic
Syntax	<code>core</code>
Parameters	None
Sub-Commands	<code>exit</code>   <code>help</code>   <code>history</code>   <code>set</code>   <code>show</code>   <code>updateimage</code>
Example	The following command example enters core configuration mode:  <code>hostname # core</code> <code>hostname (core) #</code>



**copy**

Table 3-4 copy

Description	<p>Uses Secure Copy (SCP) to scp to copy and transfer packet capture or traceback (crash) data to a remote location, providing the same authentication and level of security as an SSH transfer.</p> <p>See Also: <a href="#">diagnosis [mode]</a>; <a href="#">capture-start</a></p>
Product(s) CLI	<b>All-in-One   Collector   Core   Mac OS X Detection Engine</b>
Mode(s)	Diagnosis
Syntax	<pre>copy capture &lt;scp source_file_name username@destination_host:destination_folder&gt;   traceback all &lt;string URI as user@hostname:path&gt;</pre>
Parameters	<pre>copy capture &lt;scp remote filename_location&gt; copy traceback all &lt;path string&gt; copy traceback &lt;tab&gt; [<i>tab displays all available crash filenames</i>]</pre>
Sub-Commands	None
Example	<p>The following example copies the file "captureEth1.txt" from the local host to a remote host:</p> <pre>hostname (diagnosis)# copy capture scp captureEth1.txt admin@remotehost.edu:/some/remote/directory</pre>

**diagnosis**

Table 3-5 diagnosis

Description	<p>Enters the Diagnosis configuration and status check mode.</p> <p>See Also: <a href="#">collector [mode]</a>, <a href="#">server [mode]</a></p>
Product(s) CLI	<b>All-in-One   Collector   Core   Mac OS X Detection Engine</b>
Mode(s)	Basic
Syntax	diagnosis
Parameters	None
Sub-Commands	<pre>capture-start; copy; exit; gssreport; help; history; set (server mode); setupcheck; show (diagnosis mode); show (server mode)</pre>
Example	<p>The following example enters diagnosis configuration and status check mode:</p> <pre>hostname # diagnosis hostname (diagnosis)# ?</pre>

**exit**

Table 3-6 exit

Description	Ends the CLI session.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Core   CM   Collector   Diagnosis   Server
Syntax	<code>exit</code>
Parameters	None
Example	The following example ends the CLI session. JATP# (diagnosis) <code>exit</code> JATP#

**gssreport**

Table 3-7 gssreport

Description	Use the gssreport command to submit reports to Juniper Global Security Services (GSS), and to display the status of the current GSS report.  See Also: <a href="#">gssreport</a> ; <a href="#">diagnosis</a> [mode]
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac OS X Detection Engine</b>
Mode(s)	diagnosis
Syntax	<code>gssreport status   submit</code>
Parameters	<code>status</code> - displays the status of the current GSS report. <code>submit</code> - submits a report to Juniper ATP Appliance GSS.
Sub-Commands	None
Example	The following examples display the status of a GSS report submission:  <pre>hostname # diagnosis hostname (diagnosis)# gssreport submit Successfully started GSS report  hostname (diagnosis)# gssreport status GSS is currently enabled Last 5-minute GSS report at 2014-07-28 10:34:24.414322: successfully submitted Last hourly GSS report at 2014-07-28 10:34:24.468259: successfully submitted Last daily GSS report at 2014-07-28 10:34:28.225512: successfully submitted</pre>

[help](#)Table 3-8 [help](#)

Description	Displays information about the CLI help system.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Core   CM   Collector   Diagnosis   Server
Syntax	help
Parameters	None
Example	<p>The following example shows some of the output of the help command.</p> <pre>CONTEXT SENSITIVE HELP [?] - Display context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference.  AUTO-COMPLETION The following keys both perform auto-completion for the current command line. If the command prefix is not unique then the bell will ring and a subsequent repeat of the key will display possible completions.  [enter] - Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending part of the command line will be highlighted and explained. [tab]    - Auto-completes [space]  - Auto-completes, or if the command is already resolved inserts a space.  If "&lt;cr&gt;" is shown, that means that what you have entered so far is a complete command, and you may press Enter (carriage return) to execute it.  Use ? to learn command parameters and option:  <b>JATP (server)#</b> show f? firewall  Show the firewall configuration settings           interface <b>JATP (server)#</b> show firewall? all       Show the current iptables settings whitelist Show the iptables whitelist settings show firewall whitelist? &lt;cr&gt; show firewall whitelist</pre>

## history

Table 3-9 history

Description	Displays the current CLI session command line history.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Core   CM   Collector   Diagnosis   Server
Syntax	<b>h</b> istory
Parameters	None
Example	The following examples returns command line history for the current CLI session. JATP# history

## ifrestart

Table 3-10 ifrestart

Description	Restarts the interface driver and services using the interface.
Product(s) CLI	<b>All-in-One   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server
Syntax	ifrestart <i>eth0</i>   <i>eth1</i>
Parameters	<div>eth0                      Restarts the management network administra interface.</div> <div>eth1                      Restarts the monitoring network interface.</div>
Example	The following example restarts the <i>eth0</i> interface for the management network. <FireEye_name># ifrestart eth0

**ping**

Table 3-11 ping

Description	Sends ICMP (Internet Control Message Protocol) echo request packets to a specified host name or IP address to verify that the destination is reachable over the network.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	<b>ping</b> [-c <i>count</i> ] [-h <i>hops</i> ] [ <i>string</i> ]	
Parameters	<div>-c count</div> <div>-h hops</div> <div>string</div>	<div>Number of echo requests to send. By default, pings are continuously until you press Ctrl+C.</div> <div>Number of next hops between pings (default is 1).</div> <div>IP address, hostname or interface name used to ping device address.</div>
Example	<p>The following example sends three echo requests to the device with the IP Address 10.10.10.1</p> <pre>&lt;FireEye_name&gt;# ping -c 3 10.10.10.1  PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data. 64 bytes from 10.10.10.1: icmp_req=1 ttl=64 time=0.314 ms 64 bytes from 10.10.10.1: icmp_req=2 ttl=64 time=0.277 ms 64 bytes from v: icmp_req=3 ttl=64 time=0.274 ms  --- 10.10.10.1 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 1999ms rtt min/avg/max/mdev = 0.274/0.288/0.314/0.022 ms</pre>	

**reboot**

Table 3-12 reboot

Description	Reboots the Juniper ATP Appliance.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	<b>reboot</b>	
Parameters	None	
Example	<p>The following example reboots the system.</p> <pre>hostname# <b>reboot</b></pre>	

**restart**

Table 3-13 restart

Description	Restarts Juniper ATP Appliance services.	
-------------	--	--

Table 3-13 restart

Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	restart [all   behaviorengine   cm   collector   core   correlationengine   database   ntpserver   sshserver   staticengine   webserver]	
Parameters	all behaviorengine cm collector core correlationengine database ntpserver sshserver staticengine webserver	Restarts all Juniper ATP Appliance services. Restarts the Behavioral Analysis Engine. Restarts the Central Manager Web UI service. Restarts the Collector service. Restarts the Core Detection Engine. Restarts the Correlation Engine. Restarts the Database. Restarts the NTP server. Restarts the SSH server. Restarts the Static Analysis Engine. Restarts the web server.
Example	The following example restarts the Central manager service. JATP# restart cm	

## restore

Table 3-14 restore

Description	Restores the system configuration to the factory default settings.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	restore [support   firewall {backup   default}   hostname   network]	
Parameters	<div>support</div> <div>firewall {backup   default}</div> <div>hostname</div> <div>network</div>	<div>Restores the default support password setting for SSH remote login (set during initial installation per license). See also (server)# <a href="#">set (server mode) support</a></div> <div>Restores the firewall settings from either the previous backup, or from the default factory settings. Whitelist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the whitelist state as rules cannot be saved in that case</div> <div>Restores the system's hostname to the factory default hostname.</div> <div>Restores the IP address and DNS settings to the factory default settings.</div> <div>WARNING: This command option removes the current IP address and DNS settings, and reloads the default values for these settings.</div>
Example	<p>The following example restores the system.</p> <pre>JATP # restore</pre> <p>This next example restores the SSH login "support" password to the default.</p> <pre>JATP # restore support password</pre> <pre>Restore the default support password? (Yes/No)? yes</pre> <pre>support password was restored successfully!</pre>	

**set (core mode)**

Table 3-15 set

Description	Resets the Secondary Core UUID, if the virtual core is cloned.
Product(s) CLI	<b>Core/CM (Virtual Core)</b>
Mode(s)	Core (for Virtual Core configurations)
Syntax	set id
Sub-Commands	None
Example	<p>The following example sets the Virtual Core appliance id:</p> <pre>hostname # <b>core</b> hostname (core) # set id &lt;cr&gt;</pre>

**server**

Table 3-16 server

Description	Enters the server configuration mode.
Product(s) CLI	<b>All-in-One   Collector   Core/CM   Mac Mini Mac OS X</b>
Mode(s)	Basic
Syntax	server
Sub-Commands	<p>exit; help; history; ifrestart; ping; reboot; restore; set (server mode); show (server mode); traceroute; upgrade</p> <p>Whitelist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the whitelist state as rules cannot be saved in that case.</p>
Example	<p>The following example enters server configuration mode:</p> <pre>hostname # server hostname (server) # ?</pre>

**set system-alert (server mode)**

Table 3-17 set system-alert

Description	<p>Configure the traffic threshold and checking interval for the Collector “monitored traffic” health status.</p> <p>When the monitored traffic of a collector within the checking interval time is lower than the threshold, a system health alert is generated. You can send an email notification of the alert if email notifications of system health events are configured.</p>
Product(s) CLI	<b>All-in-One   Core CM</b>
Mode(s)	Server, See Also: <a href="#">set (diagnosis mode)</a> ; <a href="#">set (collector mode)</a> ; <a href="#">show</a>



Table 3-17 set system-alert

Syntax	<pre>set system-alert traffic &lt;integer&gt; time &lt;interval&gt;</pre> <div><b>NOTE</b> Note that both "traffic" and "time" parameters are required in order to set the threshold for both the minimum traffic and time.</div>
Parameters	<p><code>traffic</code> - the minimum traffic (in KB)</p> <p><code>interval</code> - the checking interval (in minutes)</p>
Example	<pre>JATP (server) # set system-alert traffic 100 time 30</pre> <p>This example sets the system alert such that, if the total monitored traffic of a collector within the last 30 minutes dips lower than 100KB, then a system health alert will be generated (and users will receive an email notification of the alert if email notifications are configured for system health events).</p> <p>By default this alert is disabled, and users must set the minimum traffic and interval in order to enable it. Also note that all bytes seen on Ethernet frames are counted in the traffic.</p> <p>The minimum interval for the "set system-alert traffic" time interval command is 10 minutes. If the minimum interval is set to less than 10 minutes, no alerts will be triggered.</p>

## set (server mode)

Table 3-18 set

Description	Configure the system settings.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server, See Also: <a href="#">set (diagnosis mode)</a> ; <a href="#">set (core mode)</a> ; <a href="#">show (core mode)</a>
Syntax	<pre>set [autoupdate {on   off}   cli timeout secs   clock   cm address   support {enable   disable} localmode {enable   disable}  passphrase <i>string</i>   dns   firewall {all &lt;backup   flush&gt;   whitelist}   hostname <i>string</i>   ip interface {management   alternate-exhaust}  ntpserver   password   proxy {config   enabled   remove}   timezone <i>string</i>   uipassword]</pre>
Parameters	<p><b>Note:</b> vCore for AWS does not use the following CLI commands:</p> <pre>set ip set hostname</pre> <p>[Users cannot set static IP address or change the hostname directly on an EC2 AWS instance]</p> <p>(See columns below)</p>
autoupdate {content   software} {on   off}	Turn on or off automatic product updates. set autoupdate content on
cli <i>secs</i>	Sets CLI period in seconds (0 indicates no timeout).
clock	Sets the current date and time.
cm <i>address</i>	Sets the IP address of the Central Manager and netmask using slash notation; ex: AAA.BBB.CCC.DD/X
set support {enable   disable}   {localmode}	Enables remote SSH login “support” account or localmode enable/disable.
dns	Sets DNS (or enables DHCP for DNS) for the management interface by default if interface is unspecified.

Table 3-18 set

<pre>firewall {all &lt;backup   flush&gt;   whitelist &lt;add   delete   flush&gt;}</pre>	<p>Backs up or flushes (clears) all current iptables for a firewall, or adds, deletes or flushes the current iptables whitelist-specific settings for the firewall.</p> <p>The “add” option adds an IP address to the iptables outbound whitelist.</p> <pre># set firewall whitelist add 10.1.1.1</pre>
<pre>hostname string</pre>	Sets the system's host name.
<pre>ip interface {management   alternate- exhaust} &lt;dhcp   address   netmask   gateway&gt;</pre>	Sets the IP address, netmask, or default gateway, or enables DHCP for the management or alternate-exhaust interface.
<pre>ntpserver</pre>	Sets the Network Time Protocol (NTP) server.
<pre>passphrase string</pre>	Sets the device key password; enter a string.
<pre>password</pre>	Sets a new password for the CLI administrator.
<pre>proxy {config &lt;all http&gt;   enable &lt;on off&gt;   remove &lt;all http&gt;}</pre>	<p>Config, enable/disable, or remove “all” proxy configs, or remove an HTTP-specific proxy server.</p> <p>Tip: Config the proxy for “all” protocols first, and then change HTTP proxy as needed.</p>
<pre>timezone string</pre>	Sets the timezone for the device.
<pre>uipassword</pre>	Sets a new admin password for CM Web UI access.
<pre>Examples</pre>	<p>The following example enables a proxy server.</p> <pre>JATP (server)# set proxy enable on</pre>

**set (diagnosis mode)**

Table 3-19 set

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also: <a href="#">set (server mode)</a>	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	diagnosis	
Syntax	set logging all	
Parameters	all	Sets logging for all Juniper ATP Appliance components.
	default	Sets logging to the default parameters.
	debug	Sets logging at the debug level.
	info	Sets logging at the info level.
	warning	Sets logging at the warning level.
	error	Sets logging at the error level.
	critical	Sets logging at the critical level.
Example	The following example sets the default logging level for all Juniper ATP Appliance components.  JATP(diagnosis)# set logging all	

**setupcheck**

Table 3-20 setupcheck

Description	Checks and reports on basic configuration settings and analysis pipeline setup.	
Product(s) CLI	<b>All-in-One   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	diagnosis	
Syntax	setupcheck {all   report   basic   analysis}	
Parameters	all	Checks both basic settings and analysis pipeline.
	report	Shows report of last setupcheck.
	basic	Checks basic configuration settings.
	analysis	Checks the analysis pipeline.
Example	The following example checks all basic configuration settings as well as the analysis pipeline:  JATP (diagnosis) # setupcheck all	

**show (core mode)**

Table 3-21 show

Description	Displays the guest image(s) status or whitelist statistics. See Also: <a href="#">show (server mode)</a> ; <a href="#">show (diagnostic mode)</a>
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Core
Syntax	show
Parameters	<div>images      Displays guest image update and status information.</div> <div>whitelist    Displays the name, hit count and the time of last hit of a user configured whitelist. Note that when a whitelist rule is deleted, it will be removed from the list. Updates to existing rule are not affected by the presence of the rule in the output, but hit count could increment. Further, more than one rule can be hit by a single incident.</div> <div>alternate-exhaust-interface    Displays the status of the alternate exhaust interface eth2.</div>
Example	<p>The following example demonstrates the show images command usage:</p> <pre>JATP(core)# show images</pre> <p>The following example demonstrates the show whitelist command usage:</p> <pre>JATP(core)# show whitelist</pre> <pre> JATP(core)# show whitelist Rule Name      Hit Count    Local Time of Last Hit URI1           10           Wed Sep  2 18:16:55 2015 URI2           10           Wed Sep  2 18:16:55 2015 URI3           10           Wed Sep  2 18:16:55 2015 greatfilesarey 49           Wed Sep  2 18:20:00 2015 </pre> <p>The following example shows how to get the alternate-exhaust interface (eth2) status:</p> <pre>JATP(core)# show alternate-exhaust interface</pre>

## show (diagnosis mode)

Description	Displays diagnostics information. <a href="#">See Also: show (server mode)</a>	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	diagnosis	
Syntax	<b>show</b>	
Parameters	<div>device {collectorstatus     corestatus   slavecorestatus}</div> <div>protocol {web   email}</div> <div>objects</div> <div>logging</div> <div>log error traceback</div> <div>log error last &lt;integer: number of lines to display&gt;</div>	<div>Display connected device statistics for Traffic Collector, CoreCM, or Mac Mini Detection Engine Secondary "slave core."</div> <div>Displays the session counts for network web or email protocols.</div> <div>Displays the current number of file objects.</div> <div>Displays the currently-configured logging level. <a href="#">See Also: set (diagnosis mode) logging</a></div> <div>Displays only the tracebacks (if any) generated by Juniper ATP Appliance OS process error logs. A traceback is a stack of functions that were executing when an error condition was encountered.</div> <div>Displays n [1-1000] lines of the contents of the common log file.  Example: show log error last 12</div>
Example	<p>The following example displays the connected Traffic Collector status.</p> <pre> JATP(diagnosis)# show device collectorstatus &lt;cr&gt;  JATP (diagnosis)# show device collectorstatus WEB_COLLECTOR ===== IP : 10.2.9.68 Enabled : True Last Seen : 2014-07-25 15:13:17.967000-07:00 Install Date : 2014-06-25 19:03:38-07:00 ===== IP : 10.2.20.3 Enabled : True Last Seen : 2014-07-28 11:07:42.046000-07:00 Install Date : 2013-11-14 09:25:39-08:00 </pre>	

**show (server mode)**

Table 3-22 show

Description	Display configurations and status information.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server, See Also: <a href="#">show (diagnosis mode)</a>
Syntax	show
Parameters (See tables below)	

autoupdate	Show the automatic update setting.
cli timeout	Show the CLI timeout setting.
clock	Show the current date and time.
cm	Show the Central Manager IP address.
controller	Show the driver state for interfaces.
support	Show the remote SSH login support status.
description	Show the server or system description.
devicekey	Show the device key.
devicetype	Show the device type.
dns	Show the DNS servers settings.
eula	Show the End User License Agreement.
firewall [all <  whitelist]	Show the firewall configuration settings.
hostname	Show the system's host name.
interface [management   monitoring   alternate- exhaust] See Also: show controller	Show information about the management (administrative) network interface eth0, or the monitoring interface (eth1), or the alternate-exhaust interface (eth2).
ip	Show the IP address of the management (administrative) interface eth0.  Results may show both private and public IP addresses if the AWS vCore has a public IP.

<code>name</code>	Show the server name.
<code>ntpserver</code>	Show the Network Time Protocol (NTP) server settings.
<code>proxy</code> See also <a href="#">show (collector mode)</a> for show proxy inside/outside data path	Shows the proxy configuration for the management network.
<code>stats [cpuload   disk   memory]</code>	Show system statistics:  <b>cpuload</b> shows average CPU load in the system for running processes in the last 1, 5 and 15 min intervals.  <b>disk</b> shows the disk space usage in the system.  <b>memory</b> shows the system memory usage.  <code>show stats cpuload (0.06,0.13,0.13)</code>
<code>system-alert</code>	Shows the current set system-alert settings.  Show the current timezone; example: <code>set timezone US/Pacific</code> TIP: <code>set timezone &lt;tab&gt;</code> shows options.
<code>timezone {US/Eastern   US/Central   US/ Mountain}</code>	
<code>uptime</code>	Show how long the system has been running.
<code>uuid</code>	Show the system UUID (universally unique ID).
<code>version</code>	Show Juniper ATP Appliance software and content security versions.



## Example

The following example displays information about the CoreCM server device type:

```
CoreCM(server)# show devicetype
Device type: cm, core
```

The following example requests data about the alternate-exhaust interface (eth2):

```
CoreCM(server)# show interface alternate-exhaust
```

The following example shows details about the Collector's monitoring interface (eth1):

```
CoreCM(server)# show interface monitoring
Interface: monitoring (eth1) Enabled: Yes Link: Yes
  IP Address: unknown Mask: unknown MTU: 1500
  MAC Address: 90:d6:1f:22:70:g6 Speed: 1000Mb/s Duplex:
Full
  Auto-negotiation: Yes Medium: Copper
  RX packets: 1869032424 Bytes: 1716560257902 Errors: 0
Overruns: 0
  TX packets: 409287 Bytes: 44607401 Errors: 0 Overruns: 0
  Traffic rate for the last 5 seconds/1 minute/5 minutes
    RX bits/sec:    108616/160176/442736
    RX packets/sec: 44/46/91
    TX bits/sec:    0/112/128
    TX packets/sec: 0/0/0
```

**shutdown**

Table 3-23 shutdown

Description	Shuts down the Juniper ATP Appliance server.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server
Syntax	<b>shutdown</b>
Parameters	None
Example	The following example performs a shutdown of the current device. JATP# shutdown

**traceroute**

Table 3-24 traceroute

Description	Displays the route packets trace to a host name or an IP address.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server
Syntax	traceroute
Parameters	<div> <div>-h unsigned integer</div> <div>Specifies the number of hops</div> </div> <div> <div>string</div> <div>Names the remote system to be traced.</div> </div>
Example	The following example performs a traceroute of the named device. JATP# traceroute -h 2 MacMininOSX-Engine

**upgrade**

Table 3-25 upgrade

Description	Upgrade Juniper ATP Appliance software for the Core/CM device or vCore, and all connected physical or virtual devices.
Product(s) CLI	<b>All-in-One   Core CM</b>
Mode(s)	cm
Syntax	upgrade <URI as user@hostname:path>
Parameters	<div> <div>&lt;String_URI&gt;</div> <div>Specifies the software packages to copy .from a remote location for upgrading via the Core.</div> </div>

Table 3-25 upgrade

Example	<p>The following example copies Juniper ATP Appliance software to the Core from a remote location defined by the path provided.</p> <pre>CoreCM(cm) # upgrade admin@remoteHost.edu:some/remote/directory</pre>
---------	--

**updateimage**

Table 3-26 updateimage

Description	<p>Update or correct the guest-image OS profile used by the detection and analysis behavioral engine.</p> <p>The updateimage command will update the guest images from a USB drive attached to the Juniper ATP Appliance.</p>		
Product(s) CLI	<b>All-In-One   Core-CM   Mac Mini OS X Detection Engine</b>		
Mode(s)	Core		
Syntax	updateimage		
Parameters	<table> <tr> <td>built-in</td><td>Updates the guest-image on the detection Engine.</td></tr> </table>	built-in	Updates the guest-image on the detection Engine.
built-in	Updates the guest-image on the detection Engine.		
Example	<p>The following example performs a built-in profile update for the Core detection engine.</p> <pre>JATP (core)# updateimage built-in Installing image SC-XP-20140617.img... Previous version of SC-XP-20140617.img exists. Checking integrity... Image SC-XP-20140617.img is already installed Installing image SC-W7-20140521.img... Previous version of SC-W7-20140521.img exists. Checking integrity... Image SC-W7-20140521.img is already installed</pre>		

**wizard**

Table 3-27 wizard

Description	Enters the Configuration Wizard. For Configuration Wizard commands and response, see “Configuration Wizard for the CoreCM Server” in the next section to follow command prompts and recommended responses.
Product(s) CLI	<b>All-In-One   Core/CM   Collector   Mac Mini Mac OS X</b>
Mode(s)	Basic

Table 3-27 wizard

Syntax	wizard
Parameters	None
Example	The following command starts the configuration wizard.  hostname # wizard

## Configuration Wizard for the CoreCM Server

**NOTE** Enter CTRL-C to exit the Configuration Wizard at any time. If you exit without completing the configuration, you will be prompted again whether to run the Configuration Wizard.

You may also rerun the Configuration Wizard at any time with the CLI command **wizard**.

Configuration Wizard Prompts	Customer Response Actions
<p>Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)?</p> <p>Note: Only if your DHCP response is <b>no</b>, enter the following information when prompted:</p> <ul style="list-style-type: none"> <li>a. IP address (no CIDR format)</li> <li>b. Netmask</li> <li>c. Enter a gateway IP address for this management (administrative) interface:</li> <li>d. Enter primary DNS server IP address.</li> <li>e. Do you have a secondary DNS Server (Yes/No).</li> <li>f. Do you want to enter the search domains?</li> <li>g. Enter the search domain (separate multiple search domains by space):</li> </ul> <p>Restart the administrative interface (Yes/No)?</p>	<p>We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.</p> <p>Recommended: Respond with <b>no</b>:</p> <ul style="list-style-type: none"> <li>a. Enter an IP address</li> <li>b. Enter a netmask using the form 255.255.255.0.</li> <li>c. Enter a gateway IP address.</li> <li>d. Enter the DNS server IP address</li> <li>e. If <b>yes</b>, enter the IP address of the secondary DNS server.</li> <li>f. Enter <b>yes</b> if you want DNS lookups to use a specific domain.</li> <li>g. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com</li> </ul> <p>Enter <b>yes</b> to restart with the new configuration settings applied.</p>

Enter a valid hostname.	Type a hostname when prompted; do not include the domain; for example: <b>Juniper ATP Appliance1</b>
<p>[OPTIONAL]</p> <p>If the system detects a Secondary Core with an eth3 port, then the alternate CnC exhaust option is displayed:</p> <p>Use alternate-exhaust for the analysis engine exhaust traffic (Yes/No)?</p> <p>Enter IP address for the alternate-exhaust (eth2) interface:</p> <p>Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0)</p> <p>Enter gateway IP Address for the alternate-exhaust (eth2) interface: (example:10.6.0.1)</p> <p>Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8)</p> <p>Do you have a secondary DNS server for the alternate-exhaust (eth2) interface?</p> <p>Do you want to enter the search domains for the alternate-exhaust (eth2) interface?</p> <p>Note: A complete network interface restart can take more than 60 seconds</p>	<p>Refer to “Configuring an Alternate Analysis Engine Interface” in the Juniper ATP Appliance Operator’s Guide for more information.</p> <p>Enter yes to configure an alternate eth2 interface.</p> <p>Enter the IP address for the eth2 interface.</p> <p>Enter the eth2 netmask.</p> <p>Enter the gateway IP address.</p> <p>Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface.</p> <p>Enter yes or no to confirm or deny an eth2 secondary DNS server.</p> <p>Enter yes or no to indicate whether you want to enter search domain.</p>
Regenerate the SSL self-signed certificate (Yes/No)?	<p>Enter <b>yes</b> to create a new SSL certificate for the Juniper ATP Appliance Server Web UI.</p> <p>If you decline the self-signed certificate by entering <b>no</b>, be prepared to install a certificate authority (CA) certificate.</p>
<p>Enter the following server attributes:</p> <p>Central Manager (CM) IP Address:</p> <p>Device Name: (must be unique)</p> <p>Device Description</p> <p>Device Key PassPhrase</p> <p>NOTE: Remember this passphrase and use it for all distributed devices.</p>	<p>Is this a Central Manager device?:</p> <p>Enter Yes; the system will auto-set IP 127.0.0.1 as the All-in-One IP address.</p> <p>Enter a connected Juniper ATP Appliance Collector Device Name; this identifies the Collector in the Web UI.</p> <p>Enter a device Description</p> <p>Enter a user-defined PassPhrase to be used to authenticate the Core to the Central Manager.</p>



## CHAPTER 4

# Mac OS X Engine CLI Commands

This chapter describes the CLI commands available for the Mac Mini Mac OS X “Secondary Core” detection engine device. There is no Collector Mode on this device.

---

**NOTE** You must enclose non-alphabet characters in double quotes in CLI commands.

---

### Basic Mode Commands

Use general system commands to configure the appliance, view appliance history, enter other CLI modes, obtain help with CLI syntax, and to exit the CLI session.

The general commands are:

- [core on page 66](#)
- [diagnosis on page 66](#)
- [exit on page 67](#)
- [help on page 68](#)
- [history on page 69](#)
- [server on page 72](#)
- [wizard on page 83](#)

Refer to the respective chapters in this guide to review Collector Mode, Diagnosis Mode and Server Mode commands per device-- All-in-One, Mac OS X Engine, Traffic Collector and CoreCM.

### Core Mode Commands

- [exit on page 67](#)
- [help on page 68](#)
- [history on page 69](#)
- [show \(core mode\) on page 77](#)
- [updateimage on page 81](#)

## Server Mode Commands

- [exit](#) on page 67
- [help](#) on page 68
- [history](#) on page 69
- [ifrestart](#) on page 69
- [ping](#) on page 70
- [reboot](#) on page 70
- [restart](#) on page 70
- [restore](#) on page 72
- [server](#) on page 72
- [set \(server mode\)](#) on page 74
- [show \(server mode\)](#) on page 79
- [shutdown](#) on page 81
- [traceroute](#) on page 81

## Diagnosis Mode Commands

- [capture-start](#) on page 65
- [copy](#) on page 65
- [exit](#) on page 67
- [gssreport](#) on page 67
- [help](#) on page 68
- [history](#) on page 69
- [set \(diagnosis mode\)](#) on page 76
- [setupcheck](#) on page 77
- [show \(diagnosis mode\)](#) on page 78



## Mac OS X Detection Engine CLI Commands

### capture-start

Table 4-1 capture-start

Description	Starts packet capture as a means for diagnosing and debugging network traffic and obtaining stats (not part of the Collector traffic capture engine).  See Also: <a href="#">diagnosis [mode]</a> ; <a href="#">copy</a>
Product(s) CLI	<b>All-in-One   Collector   Core   Mac OS X Detection Engine</b>
Mode(s)	Diagnosis
Syntax	capture-start
Parameters	<IP address> <interface_name>
Sub-Commands	None
Example	<p>The following example starts a packet capture process on interface eth1 for a Juniper ATP Appliance with IP address 8.8.8.8:</p> <pre>hostname # <b>diagnosis</b> hostname (diagnosis) # capture-start 8.8.8.8 eth1</pre> <p><b>NOTE</b> Note: Address 8.8.8.8 need not be a Juniper ATP Appliance. It is just a host that the capture filters on.</p>

### copy

Table 4-2 copy

Description	Uses Secure Copy (SCP) to scp to copy and transfer packet capture or traceback (crash) data to a remote location, providing the same authentication and level of security as an SSH transfer.  See Also: <a href="#">diagnosis [mode]</a> ; <a href="#">capture-start</a>
Product(s) CLI	<b>All-in-One   Collector   Core   Mac OS X Detection Engine</b>
Mode(s)	Diagnosis
Syntax	copy capture <scp source_file_name username@destination_host:destination_folder>   traceback all <string URI as user@hostname:path>
Parameters	copy capture <scp remote filename_location> copy traceback all <path string> copy traceback <tab> [tab displays all available crash filenames]
Sub-Commands	None
Example	<p>The following example copies the file "captureEth1.txt" from the local host to a remote host:</p> <pre>hostname (diagnosis) # copy capture scp captureEth1.txt admin@remotehost.edu:/some/remote/directory</pre>

**core**

Table 4-3 core

Description	Enters core mode.  See Also: basic [mode];
Product(s) CLI	<b>All-in-One   Collector   Core   Mac OS X Detection Engine</b>
Mode(s)	Basic
Syntax	core
Parameters	None
Sub-Commands	exit, help, history, show, updateimage
Example	The following command example enters core configuration mode:  hostname # core hostname (core) #

**diagnosis**

Table 4-4 diagnosis

Description	Enters the Diagnosis configuration and status check mode.  See Also: collector [mode], server [mode]
Product(s) CLI	<b>All-in-One   Collector   Core   Mac OS X Detection Engine</b>
Mode(s)	Basic
Syntax	<b>diagnosis</b>
Parameters	None
Sub-Commands	capture-start; copy; exit; gssreport; help; history; set (server mode); setupcheck; show (diagnosis mode); show (server mode)
Example	The following example enters diagnosis configuration and status check mode:  hostname # <b>diagnosis</b> hostname (diagnosis) # ?

**exit**

Table 4-5 exit

Description	Ends the CLI session.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Server   Diagnosis
Syntax	<code>exit</code>
Parameters	None
Example	<p>The following example ends the CLI session.</p> <pre>JATP# (diagnosis) exit JATP#</pre>

**gssreport**

Table 4-6 gssreport

Description	<p>Use the gssreport command to submit reports to Juniper ATP Appliance Global Security Services (GSS), and to display the status of the current GSS report.</p> <p>See Also: <a href="#">gssreport</a>; <a href="#">diagnosis</a> [mode]</p>
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac OS X Detection Engine</b>
Mode(s)	diagnosis
Syntax	<code>gssreport status   submit</code>
Parameters	<p><code>status</code> - displays the status of the current GSS report.</p> <p><code>submit</code> - submits a report to Juniper ATP Appliance GSS.</p>
Sub-Commands	None
Example	<p>The following examples display the status of a GSS report submission:</p> <pre>hostname # <b>diagnosis</b> hostname (diagnosis)# gssreport submit Successfully started GSS report  hostname (diagnosis)# gssreport status GSS is currently enabled Last 5-minute GSS report at 2014-07-28 10:34:24.414322: successfully submitted Last hourly GSS report at 2014-07-28 10:34:24.468259: successfully submitted Last daily GSS report at 2014-07-28 10:34:28.225512: successfully submitted</pre>

## help

Table 4-7 help

Description	Displays information about the CLI help system.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Server   Diagnosis
Syntax	help
Parameters	None
Example	<p>The following example shows some of the output of the help command.</p> <pre>CONTEXT SENSITIVE HELP [?] - Display context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference.</pre> <p>AUTO-COMPLETION</p> <p>The following keys both perform auto-completion for the current command line. If the command prefix is not unique then the bell will ring and a subsequent repeat of the key will display possible completions.</p> <pre>[enter] - Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending part of the command line will be highlighted and explained. [tab]   - Auto-completes [space] - Auto-completes, or if the command is already resolved inserts a space.</pre> <p>If "&lt;cr&gt;" is shown, that means that what you have entered so far is a complete command, and you may press Enter (carriage return) to execute it.</p> <p>Use ? to learn command parameters and option:</p> <pre>JATP(server) # show f? firewall Show the firewall configuration settings           interface JATP(server) # show firewall? all        Show the current iptables settings whitelist  Show the iptables whitelist settings show firewall whitelist? &lt;cr&gt; show firewall whitelist</pre>

**history**

Table 4-8 history

Description	Displays the current CLI session command line history.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Server   Diagnosis
Syntax	<code>history</code>
Parameters	None
Example	The following examples returns command line history for the current CLI session. JATP# <code>history</code>

**ifrestart**

Table 4-9 ifrestart

Description	Restarts the interface driver and services using the interface.
Product(s) CLI	<b>All-in-One   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server
Syntax	<code>ifrestart eth0   eth1</code>
Parameters	<div>eth0 Restarts the management network administra interface.</div> <div>eth1 Restarts the monitoring network interface.</div>
Example	The following example restarts the <code>eth0</code> interface for the management network. JATPMAC (server) # <code>ifrestart eth0</code>

**ping**

Table 4-10 ping

Description	Sends ICMP (Internet Control Message Protocol) echo request packets to a specified host name or IP address to verify that the destination is reachable over the network.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	ping [-c <i>count</i> ] [-h <i>hops</i> ] [ <i>string</i> ]	
Parameters	<div>-c <i>count</i></div> <div>-h <i>hops</i></div> <div><i>string</i></div>	<div>Number of echo requests to send. By default, pings are continuously until you press Ctrl+C.</div> <div>Number of next hops between pings (default is 1).</div> <div>IP address, hostname or interface name used to ping device address.</div>
Example	<p>The following example sends three echo requests to the device with the IP Address 10.10.10.1</p> <pre>&lt;FireEye_name&gt;# ping -c 3 10.10.10.1</pre> <pre> PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data. 64 bytes from 10.10.10.1: icmp_req=1 ttl=64 time=0.314 ms 64 bytes from 10.10.10.1: icmp_req=2 ttl=64 time=0.277 ms 64 bytes from v: icmp_req=3 ttl=64 time=0.274 ms  --- 10.10.10.1 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 1999ms rtt min/avg/max/mdev = 0.274/0.288/0.314/0.022 ms </pre>	

**reboot**

Table 4-11 reboot

Description	Reboots the Juniper ATP Appliance.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	reboot	
Parameters	None	
Example	<p>The following example reboots the system.</p> <pre>hostname# reboot</pre>	

**restart**

Table 4-12 restart

Description	Restarts Juniper ATP Appliance services.	
-------------	--	--

Table 4-12 restart

Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	restart [all   behaviorengine   cm   collector   core   correlationengine   database   ntpserver   sshserver   staticengine   webserver]	
Parameters	all	Restarts all Juniper ATP Appliance services.
	database	Restarts the Database.
	ntpserver	Restarts the NTP server.
	sshserver	Restarts the SSH server.
Example	<p>The following example restarts the Central manager service.</p> <pre>JATP# restart cm</pre>	

## restore

Table 4-13 restore

Description	Restores the system configuration to the factory default settings.	
Product(s) CLI	All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine	
Mode(s)	Server	
Syntax	restore [support   firewall {backup   default}   hostname   network]	
Parameters	<div><div>support</div><div>Restores the default support password setting for SSH remote login (set during initial installation per license). See also (server)# <a href="#">set (server mode) support</a></div></div> <div><div>firewall {backup   default}</div><div>Restores the firewall settings from either the previous backup, or from the default factory settings.</div></div> <div><div>hostname</div><div>Restores the system's hostname to the factory default hostname.</div></div> <div><div>network</div><div>Restores the IP address and DNS settings to the factory default settings.</div></div> <div><div></div><div>WARNING: This command option removes the current IP address and DNS settings, and reloads the default values for these settings.</div></div>	
Example	<p>The following example restores the system.</p> <pre>JATP# <b>restore</b></pre> <p>This next example restores the SSH login "support" password to the default.</p> <pre>JATP# restore support password</pre> <p>Restore the default support password? (Yes/No)? yes</p> <p>support password was restored successfully!</p>	

## server

Table 4-14 server

Description	Enters the server configuration mode.
Product(s) CLI	<b>All-in-One   Collector   Core/CM   Mac Mini Mac OS X</b>
Mode(s)	Basic
Syntax	server
Sub-Commands	exit; help; history; ifrestart; ping; reboot; restore; set (server mode); show (server mode); traceroute; updateimage



Table 4-14 server

Example	<p>The following example enters server configuration mode:</p> <pre>hostname # <b>server</b> hostname (server) # ?</pre>
---------	--

**set (server mode)**

Table 4-15 server mode

Description	Configure the system settings.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server, See Also: <a href="#">set (diagnosis mode)</a>
Syntax	<pre>set [autoupdate {on   off}   cli timeout secs   clock   cm address   support {on   off}   passphrase <i>string</i>   dns   firewall {all &lt;backup   flush&gt;   whitelist}   hostname <i>string</i>   ip interface {management   alternate-exhaust}   ntpserver   password   proxy {config   enabled   remove}   timezone <i>string</i>   uipassword]</pre>
Parameters (See table below)	
autoupdate {on   off}	Turn on or off the automatic product update feature.
cli timeout secs	Set CLI timeout period in seconds (0 = no timeout).
clock	Sets the current date and time.
cm address	Sets the IP address of the Central Manager and netmask using the slash notation; example: AAA.BBB.CCC.DD/x
set support {enable   disable}   {localmode}	Enables remote SSH login “support” account or localmode enable/disable.
passphrase <i>string</i>	Sets the device key password; enter a string.
dns	Sets the DNS servers (or enable DHCP for DNS) for the management interface eth0.
firewall {all <backup   flush>   whitelist <add   delete   flush>}	<p>Backs up or flushes (clears) all current iptables for a firewall, or adds, deletes or flushes the current iptables whitelist-specific settings for the firewall.</p> <p>The “add” option adds an IP address to the iptables outbound whitelist.</p>
NOTE: Whitelist rules rely on normal service shutdown for backup.Powering off a VM directly loses the whitelist state as rules cannot be saved in that case.	<pre># set firewall whitelist add 10.1.1.1</pre>
hostname <i>string</i>	Sets the system's host name.

Table 4-15 server mode

<code>ip interface {management   alternate- exhaust} &lt;dhcp   address   netmask   gateway}</code>	Sets the IP address, netmask, or default gateway, or enables DHCP for the management or alternate-exhaust interface.
<code>ntpserver</code>	Sets the Network Time Protocol (NTP) server.
<code>password</code>	Sets a new password for the CLI administrator.
<code>proxy {config &lt;all http&gt;   enabled &lt;on off&gt;   remove &lt;all http&gt;}</code>	Config, enable/disable, or remove “all” proxy configs, or remove an HTTP-specific proxy server. Tip: Config the proxy for “all” protocols first, and then change HTTP proxy as needed.
<code>timezone {US/ Eastern   US/ Central   US/ Mountain</code>	Show the current timezone; example: <code>set timezone US/Pacific</code> TIP: <code>set timezone &lt;tab&gt;</code> shows options.
<code>uipassword</code>	Sets a new admin password for CM Web UI access.
<hr/>	
Example	<p>The following example sets an ip address for the device management interface eth0.</p> <pre>JATP# set ip interface 10.1.1.1</pre>

**set (diagnosis mode)**

Table 4-16 set

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also: <a href="#">set (server mode)</a>	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	diagnosis	
Syntax	set logging	
Parameters	all	Sets logging for all Juniper ATP Appliance components.
	default	Sets logging to the default parameters.
	debug	Sets logging at the debug level.
	info	Sets logging at the info level.
	warning	Sets logging at the warning level.
	error	Sets logging at the error level.
	critical	Sets logging at the critical level.
Example	The following example sets the default logging level for all Juniper ATP Appliance components. <pre>JATP(diagnosis)# set logging all</pre>	

**setupcheck**

Table 4-17 setupcheck

Description	Checks and reports on basic configuration settings and analysis pipeline setup.	
Product(s) CLI	<b>All-in-One   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	diagnosis	
Syntax	setupcheck {all   report   basic   analysis}	
Parameters	all	Checks both basic settings and analysis pipeline.
	report	Shows report of last setupcheck.
	basic	Checks basic configuration settings.
	analysis	Checks the analysis pipeline.
Example	<p>The following example checks all basic configuration settings as well as the analysis pipeline:</p> <pre>JATP(diagnosis) # setupcheck all</pre>	

**show (core mode)**

Table 4-18 show

Description	Displays the guest image(s) status. See Also: <a href="#">show (server mode)</a> ; <a href="#">show (diagnostic mode)</a>	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Core	
Syntax	show	
Parameters	images	Displays guest image update and status information.
	whitelist	Displays the name, hit count and the time of last hit of a user configured whitelist. Note that when a whitelist rule is deleted, it will be removed from the list. Updates to existing rule are not affected by the presence of the rule in the output, but hit count could increment. Further, more than one rule can be hit by a single incident.
	alternate-exhaust-interface	Displays the status of the alternate exhaust interface eth2.
Example	<p>The following example demonstrates the show images command usage:</p> <pre>JATP(core) # show images</pre> <p>The following example shows how to get the alternate-exhaust interface (eth2) status:</p> <pre>JATP(core) # show alternate-exhaust interface</pre>	

Description	<p>Sets the logging levels for Juniper ATP Appliance components from diagnosis mode.</p> <p>See Also: <a href="#">show (server mode)</a></p>												
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>												
Mode(s)	diagnosis												
Syntax	show												
Parameters	<table border="0"> <tr> <td>device {collectorstatus     corestatus   slavecorestatus}</td> <td> <p>Display connected device statistics for Traffic Collector, CoreCM, or Mac Mini Detection Engine “Secondary core.”</p> <p>NOTE: Not available from the Mac Mini CLI.</p> </td> </tr> <tr> <td>protocol {web   email}</td> <td>Displays the session counts for network web or email protocols. NOTE: Not available from the Mac Mini CLI.</td> </tr> <tr> <td>objects</td> <td>Displays the current number of file objects. NOTE: Not available from the Mac Mini CLI.</td> </tr> <tr> <td>logging</td> <td>Displays the currently-configured logging level. See Also: <a href="#">set (diagnosis mode) logging</a></td> </tr> <tr> <td>log error traceback</td> <td> <p>Displays only the tracebacks (if any) generated by Juniper ATP Appliance OS process error logs. A traceback stack</p> <p>of functions that were executing when an error condition was encountered.</p> </td> </tr> <tr> <td>log error last &lt;integer: number of lines to display&gt;</td> <td>Displays n [1-1000] lines of the contents of the common log file.</td> </tr> </table>	device {collectorstatus     corestatus   slavecorestatus}	<p>Display connected device statistics for Traffic Collector, CoreCM, or Mac Mini Detection Engine “Secondary core.”</p> <p>NOTE: Not available from the Mac Mini CLI.</p>	protocol {web   email}	Displays the session counts for network web or email protocols. NOTE: Not available from the Mac Mini CLI.	objects	Displays the current number of file objects. NOTE: Not available from the Mac Mini CLI.	logging	Displays the currently-configured logging level. See Also: <a href="#">set (diagnosis mode) logging</a>	log error traceback	<p>Displays only the tracebacks (if any) generated by Juniper ATP Appliance OS process error logs. A traceback stack</p> <p>of functions that were executing when an error condition was encountered.</p>	log error last <integer: number of lines to display>	Displays n [1-1000] lines of the contents of the common log file.
device {collectorstatus     corestatus   slavecorestatus}	<p>Display connected device statistics for Traffic Collector, CoreCM, or Mac Mini Detection Engine “Secondary core.”</p> <p>NOTE: Not available from the Mac Mini CLI.</p>												
protocol {web   email}	Displays the session counts for network web or email protocols. NOTE: Not available from the Mac Mini CLI.												
objects	Displays the current number of file objects. NOTE: Not available from the Mac Mini CLI.												
logging	Displays the currently-configured logging level. See Also: <a href="#">set (diagnosis mode) logging</a>												
log error traceback	<p>Displays only the tracebacks (if any) generated by Juniper ATP Appliance OS process error logs. A traceback stack</p> <p>of functions that were executing when an error condition was encountered.</p>												
log error last <integer: number of lines to display>	Displays n [1-1000] lines of the contents of the common log file.												
Example	<p>The following example displays the connected Traffic Collector status.</p> <pre>osx-1(server)# show devicetype Device_type: slave_core.</pre>												

**show (server mode)**

Table 4-20 show

Description	Display configurations and status information.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server, See Also: <a href="#">show (diagnosis mode)</a>
Syntax	show
Parameters (See the columns below)	
autoupdate	Show the automatic update setting.
cli	Show the CLI setting.
clock	Show the current date and time.
cm	Show the Central Manager IP address.
controller	Show the driver state for interfaces.
support	Show support status.
description	Show the server or system description.
devicekey	Show the device key.
devicetype	Show the device type.
dns	Show the DNS servers settings.
eula	Show the End User License Agreement.
firewall [all <  whitelist]	Show the firewall configuration settings.
hostname	Show the system's host name.
interface [management   monitoring   alternate- exhaust]	Show information about the management (administrative) network interface eth0, or the monitoring interface (eth1), or the alternate-exhaust interface (eth2). See Also: <code>show controller</code>
ip	Show the IP address of the management (administrative) interface eth0.
name	Show the server name.
ntpserver	Show the Network Time Protocol (NTP) server settings.
proxy	Show current proxy configuration.

Table 4-20 show

stats [cpuload   disk   memory]	<p>Show system statistics:</p> <ul style="list-style-type: none"> <li>• <code>cpuload</code> shows the average CPU load in the system for running processes in the last 1, 5 and 15 minute intervals.</li> <li>• <code>disk</code> shows the disk space usage in the system.</li> <li>• <code>memory</code> shows the system memory usage.</li> </ul>
timezone	Show the current timezone.
upgrade	Show the last manual upgrade-related information.
uuid	Show the system UUID (universally unique ID).
uptime	Show how long the system has been running.
version	Show Juniper ATP Appliance software and content security versions.
Example	<p>The following example displays information about the MacOSX cpuload statistics:</p> <pre>MacOSX (server)# # show stats cpuload (0.06, 0.13, 0.13)</pre> <p>The following example requests details for the Collector's monitoring interface (eth1):</p> <pre>MacOSX(server)# show interface monitoring</pre>



**shutdown**

Table 4-21 shutdown

Description	Shuts down the Juniper ATP Appliance server.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server
Syntax	shutdown
Parameters	None
Example	The following example performs a shutdown of the current device. JATP# shutdown

**traceroute**

Table 4-22 traceroute

Description	Displays the route packets trace to a host name or an IP address.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server
Syntax	traceroute
Parameters	<div> <div>-h unsigned integer</div> <div>Specifies the number of hops</div> </div> <div> <div>string</div> <div>Names the remote system to be traced.</div> </div>
Example	The following example performs a traceroute of the named device. MacOSX1# traceroute -h 2 MacMininOSX2-Engine

**updateimage**

Description	<p>Update or correct the guest-image OS profile used by the MAC OS X detection and analysis behavioral engine.</p> <p>The updateimage command will update the guest images from a USB drive attached to the Juniper ATP Appliance.</p>
Product(s) CLI	<b>Mac Mini OS X Detection Engine</b>
Mode(s)	Core
Syntax	updateimage

Parameters	<b>built-in</b> Updates the guest-image on the Mac OSX Detection "Secondary core."
Example	<p>The following example performs a built-in Mac OS X profile update for the Mac Mini-based Secondary core detection engine.</p> <pre>MAC2(core)# updateimage built-in Installing image SC-OSX-20131003.img... Previous version of SC-OSX-20131003.img exists. Checking integrity... Latest Image SC-OSX-20131003.img is already installed Installing image SC-XP-20140617.img... Previous version of SC-XP-20140617.img exists. Checking integrity... Image SC-XP-20140617.img is already installed Installing image SC-W7-20140521.img... Previous version of SC-W7-20140521.img exists. Checking integrity... Image SC-W7-20140521.img is already installed</pre>

**upgrade**

Table 4-23 upgrade

Description	<p>Upgrade a configured Juniper ATP Appliance Mac OSX Mac Mini device. If the Mac Mini has already been upgraded to Ubuntu 14.04, this upgrade command will not be visible at the CLI because it will not be needed.</p> <p>Please note that this command will only show up for existing customers that have Mac Mini devices configured as Juniper ATP Appliance Mac OSX detection engine Secondary Cores (running Ubuntu 13.10). For new customers running Juniper ATP Appliance Release 3.2.5, each Mac Mini device is shipped with the new Ubuntu 14.04 version already installed, so in this case, the upgrade command will again not be available from the Juniper ATP Appliance Mac OSX Engine CLI.</p>	
Product(s) CLI	<b>Mac Mini OS X Detection Engine</b>	
Mode(s)	Core	
Syntax	upgrade	
Parameters	built-in	Updates the guest-image on the Mac OSX Detection “secondary core.”.
Example	<p>The following example performs a built-in Mac OS X profile update for the Mac Mini-based Secondary core detection engine.</p> <pre>MAC2 (core) # upgrade</pre>	

**wizard**

Table 4-24 wizard

Description	Enters the Configuration Wizard. For Configuration Wizard commands and response, refer to “Configuration Wizard Command Prompt Responses” in the next section to see command prompts and recommended responses.	
Product(s) CLI	<b>All-in-One   Core/CM   Collector   Mac Mini Mac OS X</b>	
Mode(s)	Basic	
Syntax	wizard	
Parameters	None	
Example	<p>The following command starts the configuration wizard.</p> <pre>hostname # <b>wizard</b></pre>	

## Configuration Wizard Command Prompt Responses

Configuration Wizard Prompts	Customer Response from the Mac Mini
<p>Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)?</p> <p>Note: Only if your DHCP response is <b>no</b>, enter the following information when prompted:</p> <ul style="list-style-type: none"> <li>a. IP address (no CIDR format)</li> <li>b. Netmask</li> <li>c. Enter a gateway IP address for this management (administrative) interface:</li> <li>d. Enter primary DNS server IP address.</li> <li>e. Do you have a secondary DNS Server (Yes/No).</li> <li>f. Do you want to enter the search domains?</li> <li>g. Enter the search domain (separate multiple search domains by space):</li> </ul> <p>Restart the administrative interface (Yes/No)?</p>	<p>We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.</p> <p>Recommended: Respond with <b>no</b>:</p> <ul style="list-style-type: none"> <li>a. Enter an IP address</li> <li>b. Enter a netmask using the form 255.255.255.0.</li> <li>c. Enter a gateway IP address.</li> <li>d. Enter the DNS server IP address</li> <li>e. If <b>yes</b>, enter the IP address of the secondary DNS server.</li> <li>f. Enter <b>yes</b> if you want DNS lookups to use a specific domain.</li> <li>g. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com</li> </ul> <p>Enter <b>yes</b> to restart with the new configuration settings applied.</p>
Enter a valid hostname.	Type a hostname when prompted; do not include the domain; for example: <b>juniperatp1</b>

Configuration Wizard Prompts	Customer Response from the Mac Mini
<p>[OPTIONAL]</p> <p>If the system detects a Secondary Core with an eth2 port, then the alternate CnC exhaust option is displayed:</p> <p>Use alternate-exhaust for the analysis engine exhaust traffic (Yes/No)?</p> <p>Enter IP address for the alternate-exhaust (eth2) interface:</p> <p>Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0)</p> <p>Enter gateway IP Address for the alternate-exhaust (eth2) interface: (example:10.6.0.1)</p> <p>Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8)</p> <p>Do you have a secondary DNS server for the alternate-exhaust (eth2) interface?</p> <p>Do you want to enter the search domains for the alternate-exhaust (eth2) interface?</p> <p>Note: A complete network interface restart can take more than 60 seconds</p>	<p>Refer to "Configuring an Alternate Analysis Engine Interface" in the Juniper ATP Appliance Operator's Guide for more information.</p> <p>Enter yes to configure an alternate eth2 interface.</p> <p>Enter the IP address for the eth2 interface.</p> <p>Enter the eth2 netmask.</p> <p>Enter the gateway IP address.</p> <p>Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface.</p> <p>Enter yes or no to confirm or deny an eth2 secondary DNS server.</p> <p>Enter yes or no to indicate whether you want to enter search domain.</p>
<p>Regenerate the SSL self-signed certificate (Yes/No)?</p>	<p>Enter <b>yes</b> to create a new SSL certificate for the Juniper ATP Appliance Server Web UI.</p> <p>If you decline the self-signed certificate by entering <b>no</b>, be prepared to install a certificate authority (CA) certificate.</p>
<p>Enter the following server attributes:</p> <p>Central Manager (CM) IP Address:</p> <p>Device Name: (must be unique)</p> <p>Device Description</p> <p>Device Key PassPhrase</p> <p>NOTE: Remember this passphrase and use it for all distributed devices!</p>	<p>Required:Enter the IP address of the Juniper ATP Appliance Server Core/CM or All-in-One.</p> <p>Enter a Juniper ATP Appliance Mac Mini or Core/CM Device Name; this identifies the Mac OS X or Core Engine in the Web UI.</p> <p>Enter a device Description</p> <p>Enter the same PassPhrase used to authenticate the Core or Mac Mini to the Central Manager.</p>



## CHAPTER 5

# Traffic Collector CLI Commands

This chapter describes the commands specific to the Juniper ATP Appliance Collector CLI. The available commands are as follows:

### Basic Mode Commands

- [collector](#) on page 89
- [diagnosis](#) on page 90
- [exit](#) on page 91
- [help](#) on page 92
- [history](#) on page 93
- [server](#) on page 97
- [wizard](#) on page 108

### Collector Mode Commands

- [exit](#) on page 91
- [help](#) on page 92
- [history](#) on page 93
- [set honeypot \(collector mode\)](#) on page 98
- [set proxy \(collector mode\)](#) on page 97
- [set proxy \(collector mode\)](#) on page 97
- [set protocols \(collector mode\)](#) on page 99
- [set traffic-filter \(collector mode\)](#) on page 102
- [show \(collector mode\)](#) on page 104

## Diagnosis Mode Commands

- [capture-start](#) on page 89
- [copy](#) on page 90
- [exit](#) on page 91
- [gssreport](#) on page 91
- [help](#) on page 92
- [history](#) on page 93
- [set \(diagnosis mode\)](#) on page 99
- [setupcheck](#) on page 103
- [show \(diagnosis mode\)](#) on page 105

## Server Mode Commands

- [exit](#) on page 91
- [help](#) on page 92
- [history](#) on page 93
- [ifrestart](#) on page 93
- [ping](#) on page 94
- [reboot](#) on page 94
- [restart](#) on page 94
- [restore](#) on page 96
- [set \(server mode\)](#) on page 100
- [show \(server mode\)](#) on page 106
- [shutdown](#) on page 108
- [traceroute](#) on page 108



## Traffic Collector CLI Commands

### capture-start

Table 5-1 capture-start

Description	Starts packet capture as a means for diagnosing and debugging network traffic and obtaining stats (not part of the Collector traffic capture engine). See Also: <a href="#">diagnosis</a> [mode]; <a href="#">collector</a> [mode]; <a href="#">copy</a>
Product(s) CLI	<b>All-In-One   Collector</b>
Mode(s)	Diagnosis
Syntax	capture-start
Parameters	<IP address> <interface_name>
Sub-Commands	None
Example	<p>The following example starts a packet capture process on interface eth1 for a Traffic Collector with IP address 8.8.8.8:</p> <pre>hostname # diagnosis hostname (diagnosis)# capture-start 8.8.8.8 eth1</pre> <p><b>NOTE</b> Note: Address 8.8.8.8 need not be a Juniper ATP Appliance. It is just a host that the capture filters on.</p>

### collector

Table 5-2 collector

Description	Enters the Collector configuration mode. See Also: <a href="#">server</a> [mode]
Product(s) CLI	<b>All-In-One   Collector</b>
Mode(s)	Basic
Syntax	collector
Parameters	None
Sub-Commands	exit; help; history; set proxy (collector mode); show (collector mode)
Example	<p>The following example enters collector configuration mode:</p> <pre>hostname # <b>collector</b> hostname (collector)# ?</pre>

**copy**

Table 5-3 copy

Description	<p>Uses Secure Copy (SCP) to scp to copy and transfer packet capture or traceback (crash) data to a remote location, providing the same authentication and level of security as an SSH transfer.</p> <p>The <code>copy traceback</code> command, upon Customer Support's request, copies the traceback files out of the box to a remote location.</p> <p>See Also: <a href="#">diagnosis [mode]</a>; <a href="#">capture-start</a></p>
Product(s) CLI	<b>All-in-One   Collector   Core-CM   Mac OSX Engine</b>
Mode(s)	Diagnosis
Syntax	<pre>copy capture &lt;scp source_file_name username@destination_host:destination_folder&gt;   traceback ALL &lt;string URI as user@hostname:path&gt;</pre>
Parameters	<pre>copy capture &lt;scp remote filename_location&gt; copy traceback all &lt;path string&gt; copy traceback &lt;tab&gt; [tab displays all available crash filenames]</pre>
Sub-Commands	None
Example	<p>The following example copies the file "captureEth1.txt" from the local host to a remote host:</p> <pre>hostname (diagnosis)# copy capture scp captureEth1.txt admin@remotehost.edu:/some/remote/directory</pre>

**diagnosis**

Table 5-4 diagnosis

Description	<p>Enters the Diagnosis configuration and status check mode.</p> <p>See Also: <a href="#">collector [mode]</a>, <a href="#">server [mode]</a></p>
Product(s) CLI	<b>All-in-One   Collector   Mac OS X Detection Engine</b>
Mode(s)	Basic
Syntax	<code>diagnosis</code>
Parameters	None
Sub-Commands	<pre>capture-start; copy; exit; gssreport; help; history; set (server mode); setupcheck; show (diagnosis mode); show (server mode)</pre>
Example	<p>The following example enters diagnosis configuration and status check mode:</p> <pre>hostname # diagnosis hostname (diagnosis)# ?</pre>

**exit**

Table 5-5 exit

Description	Ends the CLI session.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Server   Collector   Diagnosis
Syntax	<code>exit</code>
Parameters	None
Example	<p>The following example ends the CLI session.</p> <pre>JATP# (diagnosis) exit JATP#</pre>

**gssreport**

Table 5-6 gssreport

Description	<p>Use the gssreport command to submit reports to Global Security Services (GSS), and to display the status of the current GSS report.</p> <p>See Also: gssreport; diagnosis [mode]</p>
Product(s) CLI	<b>All-in-One   Collector   Mac OS X Detection Engine</b>
Mode(s)	diagnosis
Syntax	<code>gssreport status   submit</code>
Parameters	<p><code>status</code> - displays the status of the current GSS report.</p> <p><code>submit</code> - submits a report to Juniper ATP Appliance GSS.</p>
Sub-Commands	None
Example	<p>The following examples display the status of a GSS report submission:</p> <pre>hostname # <b>diagnosis</b> hostname (diagnosis)# gssreport submit Successfully started GSS report  hostname (diagnosis)# gssreport status GSS is currently enabled Last 5-minute GSS report at 2014-07-28 10:34:24.414322: successfully submitted Last hourly GSS report at 2014-07-28 10:34:24.468259: successfully submitted Last daily GSS report at 2014-07-28 10:34:28.225512: successfully submitted</pre>

## help

Table 5-7 help

Description	Displays information about the CLI help system.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Server   Collector   Diagnosis
Syntax	help
Parameters	None
Example	<p>The following example shows some of the output of the help command.</p> <pre>CONTEXT SENSITIVE HELP [?] - Display context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference.</pre> <p>AUTO-COMPLETION</p> <p>The following keys both perform auto-completion for the current command line. If the command prefix is not unique then the bell will ring and a subsequent repeat of the key will display possible completions.</p> <pre>[enter] - Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending part of the command line will be highlighted and explained. [tab]   - Auto-completes [space] - Auto-completes, or if the command is already resolved inserts a space.</pre> <p>If "&lt;cr&gt;" is shown, that means that what you have entered so far is a complete command, and you may press Enter (carriage return) to execute it.</p> <p>Use ? to learn command parameters and option:</p> <pre>JATP (server)# show f? firewall Show the firewall configuration settings interface JATP (server)# show firewall? all      Show the current iptables settings whitelist Show the iptables whitelist settings show firewall whitelist? &lt;cr&gt; show firewall whitelist</pre>

**history**

Table 5-8 history

Description	Displays the current CLI session command line history.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Basic   Server   Collector   Diagnosis
Syntax	<code>history</code>
Parameters	None
Example	The following examples returns command line history for the current CLI session. JATP# <code>history</code>

**ifrestart**

Table 5-9 ifrestart

Description	Restarts the interface driver and services using the interface.
Product(s) CLI	<b>All-in-One   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server
Syntax	<code>ifrestart eth0   eth1</code>
Parameters	<div> <div><code>eth0</code></div> <div>Restarts the management network administra interface.</div> </div> <div> <div><code>eth1</code></div> <div>Restarts the monitoring network interface.</div> </div>
Example	The following example restarts the <code>eth0</code> interface for the management network. <FireEye_name># <code>ifrestart eth0</code>

**ping**

Table 5-10 ping

Description	Sends ICMP (Internet Control Message Protocol) echo request packets to a specified host name or IP address to verify that the destination is reachable over the network.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	ping [-c count] [-h hops] [string]	
Parameters	<div>-c count</div> <div>-h hops</div> <div>string</div>	<div>Number of echo requests to send. By default, pings are continuously until you press Ctrl+C.</div> <div>Number of next hops between pings (default is 1).</div> <div>IP address, hostname or interface name used to ping device address.</div>
Example	<p>The following example sends three echo requests to the device with the IP Address 10.10.10.1</p> <pre>&lt;FireEye_name&gt;# ping -c 3 10.10.10.1</pre> <pre> PING 10.10.10.1 (10.10.10.1) 56(84) bytes of data. 64 bytes from 10.10.10.1: icmp_req=1 ttl=64 time=0.314 ms 64 bytes from 10.10.10.1: icmp_req=2 ttl=64 time=0.277 ms 64 bytes from v: icmp_req=3 ttl=64 time=0.274 ms  --- 10.10.10.1 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 1999ms rtt min/avg/max/mdev = 0.274/0.288/0.314/0.022 ms </pre>	

**reboot**

Table 5-11 reboot

Description	Reboots the Juniper ATP Appliance.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	reboot	
Parameters	None	
Example	<p>The following example reboots the system.</p> <pre>hostname# reboot</pre>	

**restart**

Table 5-12 restart

Description	Restarts Juniper ATP Appliance services.	
-------------	--	--

Table 5-12 restart

Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	restart [all   behaviorengine   cm   collector   core   correlationengine   database   ntpserver   sshserver   staticengine   webserver]	
Parameters	all	Restarts all Juniper ATP Appliance services.
	database	Restarts the Database.
	ntpserver	Restarts the NTP server.
	sshserver	Restarts the SSH server.
Example	<p>The following example restarts the Central manager service.</p> <pre>JATP# restart cm</pre>	

## restore

Table 5-13 restore

Description	Restores the system configuration to the factory default settings.	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	Server	
Syntax	restore [support   firewall {backup   default}   hostname   network]	
Parameters	<div>support</div> <div>firewall {backup   default}</div> <div>hostname</div> <div>network</div>	<div>Restores the default support password setting for SSI remote login (set during initial installation per license) See also (server)# <a href="#">set (server mode) support</a></div> <div>Restores the firewall settings from either the previous backup, or from the default factory settings.</div> <div>Restores the system's hostname to the factory default hostname.</div> <div>Restores the IP address and DNS settings to the factory default settings.</div> <div>WARNING: This command option removes the current IP address and DNS settings, and reloads the default values for these settings.</div>
Example	<p>The following example restores the system.</p> <pre>JATP# restore</pre> <p>This next example restores the SSH login "support" password to the default.</p> <pre>JATP# restore support password</pre> <p>Restore the default support password? (Yes/No)? yes</p> <p>support password was restored successfully!</p>	



**server**

Table 5-14 server

Description	Enters the server configuration mode. See Also: <a href="#">collector</a>
Product(s) CLI	<b>All-in-One   Collector   Core/CM   Mac Mini Mac OS X</b>
Mode(s)	Basic
Syntax	<code>server</code>
Sub-Commands	<code>exit; help; history; ifrestart; ping; reboot; restore; set (server mode); show (server mode)</code>
Example	The following example enters server configuration mode:  <pre>hostname # <b>server</b> hostname (server) # ?</pre>

**set proxy (collector mode)**

Table 5-15 set proxy

Description	<p>Sets an Inside or Outside data path proxy from collector mode.</p> <p>Deploy Traffic Collectors in locations where the monitoring interface is (1) placed “outside” between the proxy and the egress network for customer environments in which the proxy supports XFF (X-Forwarded-For), or (2) [the more typical deployment scenario], the Collector is placed between the proxy and the internal network using FQDN (if available) to identify the threat source for all types of incidents (“inside” proxy). When configured, the Juniper ATP Appliance Traffic Collector will monitor all traffic and correctly identify source and destination hosts for each link in the kill chain wherever the data allows for it.</p> <p>Note that if the “X-Forwarded-For” header is provided in the HTTP request, detection will identify threat targets when deployed outside of the proxy (customers can choose to disable the XFF feature in the proxy setting, if desired).</p> <p>See Also: <a href="#">set (server mode)</a>; <a href="#">set (diagnosis mode)</a></p> <hr/> <p><b>NOTE</b> The mitigation IP address of a CNC server is not be available for Inside proxy deployments. When a Juniper ATP Appliance is deployed behind a proxy, the Mitigation-&gt; Firewall page in the Juniper ATP Appliance Central Manager Web UI (which typically displays the CNC server IP address to mitigate) will be empty. The destination IP address of any callback is made to the proxy server ip address, so it is not relevant to display the proxy server IP address on the Mitigation-&gt;Firewall page.</p> <hr/>
Product(s) CLI	<b>All-in-One   Collector</b>
Mode(s)	collector
Syntax	<pre>set proxy inside {add &lt;proxy IP address&gt; &lt;proxy port&gt;   remove &lt;proxy IP address&gt; &lt;proxy port&gt;  set proxy outside {add &lt;proxy IP address&gt;   remove &lt;proxy IP address&gt;</pre>

Table 5-15 set proxy

Parameters	inside	Sets the inside proxy IP addresses
	outside	Sets the outside proxy IP addresses
	add	Adds a proxy configuration.
	remove	Removes a proxy configuration.
Example	The following example sets an inside data path proxy: JATP(collector)# set proxy inside 10.1.1.1 53	
	The following example sets an outside data path proxy: JATP(collector)# set proxy outside 10.2.1.1	

**set honeypot (collector mode)**

Table 5-16 set honeypot

Description	<p>Enables and disables the SSH-Honeypot feature for a Traffic Collector.</p> <p>A honeypot can be deployed within a customer network to detect network activity generated by malware attempting to infect or attack other machines in a local area network. These attempted SSH logins can be used to supplement detection of lateral spread.</p> <p>There are two parameters that can be set for a honeypot:</p> <ul style="list-style-type: none"> <li>• Enable/disable a honeypot</li> <li>• Set a Static IP (IP, mask, and gateway) or DHCP of a publicly addressable interface</li> </ul> <p>See Also: <code>show honeypot</code> command in <a href="#">show (collector mode)</a></p>
Product(s) CLI	<b>All-in-One   Collector</b>
Mode(s)	collector
Syntax	<pre>(collector)# set honeypot ssh-honeypot enable dhcp (collector)# set honeypot ssh-honeypot enable address (IP address) netmask (subnet IP) gateway (IP address) (collector):# set honeypot ssh-honeypot disable</pre>
Example	<p>The following example enables the SMB parser for lateral detections:</p> <pre>(collector)# set honeypot ssh-honeypot enable address 1.2.3.4 netmask 255.255.0.0 gateway 1.2.3.1</pre> <p><b>NOTE</b> The static IP configuration does not require configuring DNS. Honeypots do not require a DNS server at this time.</p>

**set (diagnosis mode)**

Table 5-17 set

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also: <a href="#">set (server mode)</a> ; <a href="#">set proxy (collector mode)</a>	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	diagnosis	
Syntax	set logging	
Parameters	<div>all</div> <div>default</div> <div>debug</div> <div>info</div> <div>warning</div> <div>error</div> <div>critical</div>	<div>Sets logging for all Juniper ATP Appliance components.</div> <div>Sets logging to the default parameters</div> <div>Sets logging at the debug level.</div> <div>Sets logging at the info level.</div> <div>Sets logging at the warning level.</div> <div>Sets logging at the error level.</div> <div>Sets logging at the critical level.</div>
Example	<p>The following example sets the default logging level for all Juniper ATP Appliance components.</p> <pre>JATP# set logging all</pre>	

**set protocols (collector mode)**

Table 5-18 set protocols

Description	Enables and disables the HTTP or SMB parser for a Traffic Collector. See Also: <a href="#">show protocols</a> command in <a href="#">show (collector mode)</a>	
Product(s) CLI	<b>All-in-One   Collector</b>	
Mode(s)	collector	
Syntax	(collector)# set protocols {http [on off]   smb [on off]}	
Example	<p>The following example enables the SMB parser for lateral detections:</p> <pre>hostname (collector) set protocols smb on</pre>	

## set (server mode)

Table 5-19 set

Description	Configure the system settings.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server, See Also: <a href="#">set (diagnosis mode)</a> ; set proxy (collector mode)
Syntax	<pre>set [autoupdate {on   off}   cli timeout <i>secs</i>   clock   cm address   support {on   off}   passphrase <i>string</i>   dns   firewall {all &lt;backup   flush&gt;   whitelist}   hostname <i>string</i>   ip {interface   dhcp   address   netmask   gateway}   ntpserver   password   proxy {config   enabled   remove}   timezone <i>string</i>   uipassword]</pre>
Parameters (See columns below)	
autoupdate {software  content} {on off}	<p>Turn on or off the automatic product update feature.</p> <pre>autoupdate {software  content} {on off}</pre> <p>example: set autoupdate content on</p>
cli timeout secs	Set CLI timeout period in seconds (0 indicates no timeout).
clock	Sets the current date and time.
cm address	Sets the IP address of the Central Manager and netmask using the slash notation; example: AAA.BBB.CCC.DD/x
set support {enable   disable}   {localmode}	Enables remote SSH login “support” account or localmode enable/disable.
passphrase string	Sets the device key password; enter a string.
dns	Sets the DNS servers (or enable DHCP for DNS) for the management interface eth0.
firewall {all <backup   flush>   whitelist <add   delete   flush>}	<p>Backs up or flushes (clears) all current iptables for a firewall, or adds, deletes or flushes the current iptables whitelist-specific settings for the firewall.</p> <p>The “add” option adds an IP address to the iptables outbound whitelist.</p> <pre># set firewall whitelist add 10.1.1.1</pre> <p>Whitelist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the whitelist state as rules cannot be saved in that case</p>
hostname string	Sets the system's host name.
ip {interface   dhcp   address   netmask  gateway}	Sets the IP address, netmask, or default gateway, or enables DHCP for the management interface eth0.
ntpserver	Sets the Network Time Protocol (NTP) server.
password	Sets a new password for the CLI administrator.

Table 5-19 set

<pre>proxy {config &lt;all http&gt;   enabled &lt;on off&gt;   remove &lt;all http&gt;}</pre>	<p>Config, enable/disable, or remove “all” proxy configs, or remove an HTTP-specific proxy server.</p> <p>Tip: Config the proxy for “all” protocols first, and then change HTTP proxy as needed for management network.</p>
<pre>timezone</pre>	<p>Show the current timezone; example:</p> <pre>set timezone {US/Pacific US/Eastern   US/Central   US/Mountain}</pre> <p>TIP: <code>set timezone &lt;tab&gt;</code> shows all options</p>
<pre>uipassword</pre>	<p>Sets a new Central Manager Web UI admin password.</p>
Example	<p>The following example sets an ip address for the device management interface eth0.</p> <pre>JATP# set ip interface 10.1.1.1</pre>

**set traffic-filter (collector mode)**

Table 5-20 set traffic-filter

Description	<p>Sets traffic filter rules to avoid analysis on a set of configured traffic, which cannot be made retroactive; for example: any analysis skipped as a result of the filtering cannot be reversed. This command can be applied to an entire network/subnet/CIDR range.</p> <p>See Also: <a href="#">set (server mode)</a>; show (diagnosis mode) [show traffic-filter]</p>		
Product(s) CLI	<b>All-in-One   Collector</b>		
Mode(s)	collector		
Syntax	<pre>set traffic-filter {add &lt;rule_name&gt; &lt;domain&gt; &lt;source- address&gt; &lt;destination-address&gt; &lt;source-port&gt; &lt;destination-port&gt; &lt;protocol&gt;   remove &lt;rule_name&gt;}</pre>		
Parameters	<table border="0"> <tr> <td style="vertical-align: top;"> <pre>traffic-filter add &lt;RuleString&gt;&lt;Dom ainString&gt;&lt;sourc e- address&gt;&lt;destina tion-address&gt; &lt;source-port&gt; &lt;destination- port&gt; &lt;protocol&gt;</pre> </td><td style="vertical-align: top;"> <p>Adds a traffic filter rule where:</p> <p>“RuleString” is the name of the rule</p> <p>“DomainString” is the domain to filter out</p> <p>“source-address” is the source IPv4 address or network (CIDR)</p> <p>“destination-address” is the destination IPv4 address or network (CIDR)</p> <p>“source-port” is the source port number (0-65535)</p> <p>“destination-port” is the destination port number (0-65535)</p> <p>“protocol” is the protocol type: either IP, TCP, UDP or HTTP</p> </td></tr> </table>	<pre>traffic-filter add &lt;RuleString&gt;&lt;Dom ainString&gt;&lt;sourc e- address&gt;&lt;destina tion-address&gt; &lt;source-port&gt; &lt;destination- port&gt; &lt;protocol&gt;</pre>	<p>Adds a traffic filter rule where:</p> <p>“RuleString” is the name of the rule</p> <p>“DomainString” is the domain to filter out</p> <p>“source-address” is the source IPv4 address or network (CIDR)</p> <p>“destination-address” is the destination IPv4 address or network (CIDR)</p> <p>“source-port” is the source port number (0-65535)</p> <p>“destination-port” is the destination port number (0-65535)</p> <p>“protocol” is the protocol type: either IP, TCP, UDP or HTTP</p>
<pre>traffic-filter add &lt;RuleString&gt;&lt;Dom ainString&gt;&lt;sourc e- address&gt;&lt;destina tion-address&gt; &lt;source-port&gt; &lt;destination- port&gt; &lt;protocol&gt;</pre>	<p>Adds a traffic filter rule where:</p> <p>“RuleString” is the name of the rule</p> <p>“DomainString” is the domain to filter out</p> <p>“source-address” is the source IPv4 address or network (CIDR)</p> <p>“destination-address” is the destination IPv4 address or network (CIDR)</p> <p>“source-port” is the source port number (0-65535)</p> <p>“destination-port” is the destination port number (0-65535)</p> <p>“protocol” is the protocol type: either IP, TCP, UDP or HTTP</p>		
Example	<p>The following example add a traffic filter rule to the Traffic Collector.</p> <pre>JATP-collector02(collector)# set traffic-rule add CustomRule2 headqrts.example.com 10.2.00/16 20.0.0.2 90 120 tcp</pre> <p>where destination-address is 20.0.0.2, destination-port is 120, protocol is tcp, source-address is 10.2.0.0/16 and source-port is 90 (in our example).</p>		

**set traffic-monitoring (for JATP700 Appliances only) (collector mode)**

Table 5-21 set traffic-monitoring

Description	Sets the traffic monitoring interface on the JATP700
Product(s) CLI	<b>All-in-One   Collector</b>
Mode(s)	collector

Table 5-21 set traffic-monitoring

Syntax	# set traffic-monitoring-ifc 1gb_ifc Set the traffic monitoring interface to be the 1G interface.
	# set traffic-monitoring-ifc 10gb_ifc Set the traffic monitoring interface to be the 10G interface.
	<b>NOTE</b> After making an interface type change, the system must be rebooted for the change to take effect.

## setupcheck

Table 5-22 setupcheck

Description	Checks and reports on basic configuration settings and analysis pipeline setup.	
Product(s) CLI	<b>All-in-One   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	diagnosis	
Syntax	setupcheck {all   report   basic   analysis}	
Parameters	all	Checks both basic settings and analysis pipeline.
	report	Shows report of last setupcheck.
	basic	Checks basic configuration settings.
	analysis	Checks the analysis pipeline.
Example	<p>The following example checks all basic configuration settings as well as the analysis pipeline:</p> <p>JATP (diagnosis) # setupcheck all</p>	

**show (collector mode)**

Table 5-23 show

Description	Displays the Traffic Collector current traffic filters and the current XFF status (enabled or disabled)	
Product(s) CLI	<b>All-in-One   Collector</b>	
Mode(s)	Collector	
Subcommands	traffic-filter   proxy   honeypot	
Syntax	show	
Parameters	<div>traffic-filter</div> <div>protocols</div> <div>proxy {inside   outside}</div> <div>honeypot</div>	<div>Shows all traffic filter rules.</div> <div>Shows current HTTP or SMB protocol parser settings.</div> <div>Shows Traffic Collector proxy for inside or outside configurations. See also show proxy: <a href="#">show (server mode)</a></div> <div>Shows the current honeypot configuration. show honeypot ssh-honeypot</div>
Example	<p>The following example displays the current Collector proxy inside settings:</p> <pre>collector02(collector)# show proxy inside Proxy IPs: 10.1.1.1</pre> <p>The following example displays the current traffic filter:</p> <pre>collector02 (collector)# show traffic-filter Name: CustomRule2, Domain: headqtrs.example.com</pre> <p>The following example displays the current SMB protocol parser setting:</p> <pre>collector02 (collector)# show protocols</pre>	



**show (diagnosis mode)**

Table 5-24 show

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also: <a href="#">show (server mode)</a> ; <a href="#">show (collector mode)</a>	
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>	
Mode(s)	diagnosis	
Syntax	show	
Parameters	<div> <div>device {collectorstatus     corestatus   slavecorestatus}</div> <div>Display connected device statistics for Traffic Collector, Core, or Mac Mini Detection Engine “Secondary core.”  NOTE: Not available from the Collector CLI.</div> </div> <div> <div>protocol {web   email}</div> <div>Displays the session counts for network web or email protocols. NOTE: Not available from the Collector CLI.</div> </div> <div> <div>objects</div> <div>Displays the current number of file objects. NOTE: Not available from the Collector CLI.</div> </div> <div> <div>logging</div> <div>Displays the currently-configured logging level. See Also: <a href="#">set (diagnosis mode) logging</a></div> </div> <div> <div>log error traceback</div> <div>Displays only the tracebacks (if any) generated by Juniper ATP Appliance OS process error logs. A traceback is a stack of functions that were executing when an error condition was encountered.  NOTE: Not available from the Collector CLI.</div> </div> <div> <div>log error last &lt;integer: number of lines to display&gt;</div> <div>Displays n [1-1000] lines of the contents of the common log file. NOTE: Not available from the Collector CLI.  Example: show log error last 12</div> </div>	
Example	<p>The following example displays the connected Traffic Collector status.</p> <pre> JATP(diagnosis)# show device collectorstatus &lt;cr&gt;  JATP (diagnosis)# show device collectorstatus WEB_COLLECTOR ===== IP : 10.2.9.68 Enabled : True Last Seen : 2014-07-25 15:13:17.967000-07:00 Install Date : 2014-06-25 19:03:38-07:00 ===== IP : 10.2.20.3 Enabled : True Last Seen : 2014-07-28 11:07:42.046000-07:00 Install Date : 2013-11-14 09:25:39-08:00 </pre>	

**show (server mode)**

Table 5-25 show

Description	Display configurations and status information.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server, See Also: <a href="#">show (collector mode)</a> ; <a href="#">show (diagnosis mode)</a>
Syntax	<code>show</code>
Parameters (See columns below)	
<code>autoupdate</code>	Show the automatic update setting.
<code>cli timeout</code>	Show the CLI timeout setting.
<code>clock</code>	Show the current date and time.
<code>cm</code>	Show the Central Manager IP address.
<code>controller</code>	Show the driver state for interfaces.
<code>support</code>	Show the remote SSH login support status.
<code>description</code>	Show the server or system description.
<code>devicekey</code>	Show the device key.
<code>devicetype</code>	Show the device type.
<code>dns</code>	Show the DNS servers settings.
<code>eula</code>	Show the End User License Agreement.
<code>firewall [all &lt;  whitelist]</code>	Show the firewall configuration settings.
<code>hostname</code>	Show the system's host name.
<code>interface</code>	Show information about the management (administrative) network interface eth0 and the monitoring interface eth1.
<code>ip</code>	Show the IP address of the management (administrative) interface eth0. Results may show both private and public IP addresses if the AWS vCore has a public IP.
<code>name</code>	Show the server name.
<code>ntpserver</code>	Show the Network Time Protocol (NTP) server settings.
<code>proxy</code>	Show the current proxy configuration.
<code>uuid</code>	Show the system UUID (universally unique ID).

Table 5-25 show

<code>stats [cpuload   disk   memory]</code>	<div>Show system statistics:<ul style="list-style-type: none"><li>• <code>cpuload</code> shows the average CPU load in the system</li><li>• <code>disk</code> shows the disk space usage in the system.</li><li>• <code>memory</code> shows the system memory usage.</li></ul><pre># show stats cpuload (0.06, 0.13, 0.13)</pre></div>
<code>timezone</code>	Show the current timezone.
<code>uptime</code>	Show how long the system has been running.
<code>version</code>	Show software and content security versions.
Example	<div>The following example displays information about the All-in-One server device type:<pre>All-in-One(server)# show devicetype Device type: cm, core, web_collector.</pre></div>

**shutdown**

Table 5-26 shutdown

Description	Shuts down the Juniper ATP Appliance server.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server
Syntax	shutdown
Parameters	None
Example	The following example performs a shutdown of the current device.  JATP# shutdown

**traceroute**

Table 5-27 traceroute

Description	Displays the route packets trace to a host name or an IP address.
Product(s) CLI	<b>All-in-One   Collector   Core CM   Mac Mini OS X Detection Engine</b>
Mode(s)	Server   Collector
Syntax	traceroute
Parameters	<div> <div>-h unsigned integer</div> <div>Specifies the number of hops</div> </div> <div> <div>string</div> <div>Names the remote system to be traced.</div> </div>
Example	The following example performs a traceroute of the named device.  JATP# traceroute -h 2 8.8.8.8

**wizard**

Table 5-28 wizard

Description	Enters the Configuration Wizard. For Configuration Wizard commands and response, see “Configuration Wizard Command Prompt Progressions” in the next section to see command prompts and recommended responses.
Product(s) CLI	<b>All-in-One   Core/CM   Collector   Mac Mini Mac OS X</b>
Mode(s)	Basic
Syntax	wizard
Parameters	None
Example	The following command starts the configuration wizard. See “Configuration Wizard Command Prompt Progressions” in the next section.  hostname # wizard

See wizard command prompt progression, as follows:

## Configuration Wizard Command Prompt Progressions

Table 5-29 Configuration Wizard

Configuration Wizard Prompts	Customer Response from Collector
<p>Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)?</p> <p>Note: Only if your DHCP response is <b>no</b>, enter the following information when prompted:</p> <ul style="list-style-type: none"> <li>a. IP address (no CIDR format)</li> <li>b. Netmask</li> <li>c. Enter a gateway IP address for this management (administrative) interface:</li> <li>d. Enter primary DNS server IP address.</li> <li>e. Do you have a secondary DNS Server (Yes/No).</li> <li>f. Do you want to enter the search domains?</li> <li>g. Enter the search domain (separate multiple search domains by space):</li> </ul> <p>Restart the administrative interface (Yes/No)?</p>	<p>We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.</p> <p>Recommended: Respond with <b>no</b>:</p> <ul style="list-style-type: none"> <li>a. Enter an IP address</li> <li>b. Enter a netmask using the form 255.255.255.0.</li> <li>c. Enter a gateway IP address.</li> <li>d. Enter the DNS server IP address</li> <li>e. If <b>yes</b>, enter the IP address of the secondary DNS server.</li> <li>f. Enter <b>yes</b> if you want DNS lookups to use a specific domain.</li> <li>g. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com</li> </ul> <p>Enter <b>yes</b> to restart with the new configuration settings applied.</p>
Enter a valid hostname.	Type a hostname when prompted; do not include the domain; for example: <b>juniperatp1</b>
Regenerate the SSL self-signed certificate (Yes/No)?	Not applicable to Collector.
<p>Enter the following server attributes:</p> <p>Central Manager (CM) IP Address:</p> <p>Device Name: (must be unique)</p> <p>Device Description</p> <p>Device Key PassPhrase</p> <p>NOTE: Remember this passphrase and use it for all distributed devices!</p>	<p>Required: Enter the IP address of the Juniper ATP Appliance Server All-in-One CM or CoreCM to which you are connecting [another] Collector in order to register with and view the Collector in the CM Web UI.</p> <p>Enter the Juniper ATP Appliance Collector Device Name; this identifies the Collector in the Web UI.</p> <p>Enter a device Description</p> <p>Enter the same PassPhrase used to authenticate the Collector to the Central Manager.</p>

**NOTE** Enter CTRL-C to exit the Configuration Wizard at any time. If you exit without completing the



## CHAPTER 6

# Glossary of Terms

Alternate Exhaust Interface	An eth2 interface configured (optionally) to contain analysis engine CnC traffic off the management network (eth0).
Anti-SIEM	A Juniper ATP Appliance Advanced Threat Analytics (ATA) feature that allows for more detailed endpoint and log ingestion handling, management and reporting; includes Active Directory, Splunk and Direct Log Ingestion options.
AWS	Amazon Web Services and EC2 management console from which Juniper ATP Appliance administrators can configure vCore AMI images.
Blacklist	A list or register of entities to be denied a specified access or privilege. During detection engine analysis, when content matches any pattern on the blacklist, the content is deemed malicious and therefore an alert or block action is enacted immediately.
Collector	Juniper ATP Appliance's Traffic inspection and object collection mechanism
CnC server	Command and control server that directs the operation of a botnet.
CLI	Command-line interface. The Juniper ATP Appliance has a CLI interface for administering the appliance.
CM	The Juniper ATP Appliance Central Manager component that has a web-based graphical user interface.
Darkspace	Currently unused address space.
DHCP	Dynamic Host Configuration Protocol.
DMZ	Demilitarized zone. An area of the network where systems have direct access to the Internet or an external network.
DNS	Domain Name Service.
Event	Indicates a type of security intrusion or attack.
Greylist	Greylists provide control over the priority of workorders for known IP addresses and URLs. Greylists contain files that contain either URLs or IP addresses and are used by the Juniper ATP Appliance analysis engines to check if the specified URLs or IP addresses contain a malicious rule match.

GUI	Graphical user interface. The Juniper ATP Appliance uses a web-based GUI for managing the appliance.
Known botnet server bot command	Events that are triggered when the appliance sees any of the common IRC bot commands or detects any communication sent to known botnet servers.
Lateral Detection	East-west detection of malware within the enterprise spread from endpoint host to host.
Malware	Malicious software used by attackers to disrupt, control, steal, cause data loss, spy upon, or gain unauthorized access to computer systems.
NTP	Network Time Protocol.
OS-anomaly	Events that indicate modification of the operating system.
OSPF	Open Shortest Path First. A protocol that computes an optimal path for traffic in a TCP/IP network.
Sandbox mode	A mode in which malware is permitted to run, but results of the malware action are restricted to the virtual machine and not permitted to escape.
SNMP	Simple Network Management Protocol.
Spyware	A type of malware installed on computers that collects small pieces of information about user(s) it is spying on.
SSL	Secure Sockets Layer.
TLS	Transport Layer Security.
VLAN	Virtual Local Area Network.
VM	Virtual Machine. A software program that runs an instance of an operating system. The operating system runs on top of a program that emulates a hardware system.
Worm	A self-replicating malware program that uses a computer network to send copies of itself to other computers. This may be done without any user intervention.
Zero-day attack	An attack by malware that exploits unknown or newly discovered vulnerabilities in software before they become known or before security patches are applied to fix them