Juniper NETWORKS | Engineering Simplicity

CLI Command Reference Guide

Published

2023-02-01

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

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.

CLI Command Reference Guide

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 documentation 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 https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to learn about the JATP CLI commands for system configuration and status monitoring.

1

CHAPTER

CLI Command Reference Guide

Preface

IN THIS SECTION

This preface contains the following sections:

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:

- "Introduction" on page 4—Includes an overview of CLI usage, CLI Modes and information about how to access the Juniper ATP Appliance Command Line Interface.
- "All-in-One CLI Commands" on page 15—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.
- "Core/CM Server CLI Commands" on page 59—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.

- "Mac OS X Engine CLI Commands" on page 105—Provides information about Mac Mini Mac OS X Detection Engine-specific commands for configuration and status monitoring.
- "Traffic Collector CLI Commands" on page 137—Provides information about the Juniper ATP Appliance Traffic Collector commands available for identifying, monitoring, and configuring distributed Collector hardware, software and virtual appliances.
- "Glossary of Terms" on page 174—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 1: Table 4-1 Typographical Conventions

Convention	Meaning	Example
courier font Click	Coding examples and text to be entered at the command prompt A left-mouse button click.	Enter the following command: server set dns 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 HTTP API Reference Guide— Provides Juniper ATP Appliance HTTP API functions and information about usage.

Introduction

IN THIS SECTION

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 THIS SECTION

Hardware Appliance CLI Access via Keyboard and Monitor

1. Connect the end of the keyboard cable to any of the USB ports on the back panel of the appliance.

2. Connect the end of the video monitor cable to the VGA port on the back panel of the appliance.

3. 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.

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

Configuration Wizard Command Prompt Progressions

IN THIS SECTION

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 All-in-One	Customer Response from Core or Mac Mini	Customer Response from Collector

Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)? **NOTE**: Only if your DHCP response is no,enter the following information when prompted: 1. IP address 2. Netmask 3. Enter a gateway IP address for this management (administrative) interface: 4. Enter primary DNS server IP address. 5. Do you have a secondary DNS Server (Yes/No). 6. Do you want to enter the search domains? 7. Enter the search domain (separate multiple search domains by space): Restart the administrative interface (Yes/No)?	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred. Recommended: Respond with no: 1. Enter an IP address 2. Enter a netmask using the form 255.255.255.0. 3. Enter a gateway IP address. 4. Enter the DNS server IP address 5. If yes, enter the IP address of the secondary DNS server. 6. Enter yes if you want DNS lookups to use a specific domain. 7. Enter space domain(s) separated by spaces; for example: example.com lan.com dom2.com Enter yes to restart with the new configuration settings applied.	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred. Recommended: Respond with no: 1. Enter an IP address 2. Enter a netmask using the form 255.255.255.0. 3. Enter a gateway IP address. 4. Enter the DNS server IP address 5. If yes, enter the IP address of the secondary DNS server. 6. Enter yes if you want DNS lookups to use a specific domain. 7. Enter space domain(s) separated by spaces; for example: example.com lan.com dom2.com Enter yes to restart with the new configuration settings applied.	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred. Recommended: Respond with no: 1. Enter an IP address 2. Enter a netmask using the form 255.255.255.0. 3. Enter a gateway IP address. 4. Enter the DNS server IP address 5. If yes, enter the IP address of the secondary DNS server. 6. Enter yes if you want DNS lookups to use a specific domain. 7. Enter space domain(s) separated by spaces; for example: example.com lan.com dom2.com Enter yes to restart with the new configuration settings applied.

Enter a valid hostname (enter a unique name) **NOTE**: Only alpha-numeric characters and hyphens (in the middle of the hostname) are allowed.	Type a hostname when prompted; do not include the domain; for example: **juniperatp1**	Type a hostname when prompted; do not include the domain; for example: **juniperatp1**	Type a hostname when prompted; do not include the domain; for example: **juniperatp1**

[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)? Enter IP address for the alternate-exhaust (eth2) interface: Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0) Enter gateway IP Address for the alternate-exhaust (eth2) interface: (example:10.6.0.1) Enter primary DNS server IP Address for the alternateexhaust (eth2) interface: (example: 8.8.8.8) Do you have a secondary DNS server for the alternate-exhaust (eth2) interface? Do you want to enter the search domains for the alternateexhaust (eth2) interface? **NOTE**: A complete network interface restart can take more than 60 seconds	Refer to “Configuring an Alternate Analysis Engine Interface” in the Juniper ATP Appliance Operator’s Guide for more information. Enter yes to configure an alternate eth2 interface. Enter the IP address for the eth2 interface. Enter the eth2 netmask. Enter the gateway IP address. Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface. Enter yes or no to confirm or deny an eth2 secondary DNS server. Enter yes or no to indicate whether you want to enter search domain.	Refer to “Configuring an Alternate Analysis Engine Interface” in the Juniper ATP Appliance Operator’s Guide for more information. Enter yes to configure an alternate eth2 interface. Enter the IP address for the eth2 interface. Enter the eth2 netmask. Enter the gateway IP address. Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface. Enter yes or no to confirm or deny an eth2 secondary DNS server. Enter yes or no to indicate whether you want to enter search domain.	[Traffic Collectors do not send or receive Core analysis engine CnC network traffic, so no eth2 interface is needed.]

Regenerate the SSL self-signed certificate (Yes/ No)?	Enter yes to create a new SSL certificate for the Juniper ATP Appliance Server Web UI. If you decline the selfsigned certificate by entering no, be prepared to install a certificate authority (CA) certificate.	Enter yes to create a new SSL certificate for the Juniper ATP Appliance Server Web UI. If you decline the selfsigned certificate by entering no, be prepared to install a certificate authority (CA) certificate.	Not applicable to Collector.
Enter the following server attributes: Is this a Central Manager device: Device Name: (must be unique) Device Description Device Key PassPhrase **NOTE**: Remember this passphrase and use it for all distributed devices!	Enter Yes; the system will auto-set IP 127.0.0.1 as the All-in- One IP address. Enter the Juniper ATP Appliance Collector Host Name; this identifies the Collector in the Web UI. Enter a device Description Enter a user-defined PassPhrase to be used to authenticate the Core to the Central Manager.	Enter Yes; the system will auto-set IP 127.0.0.1 as the All-in- One IP address. Enter the Juniper ATP Appliance Collector Host Name; this identifies the Collector in the Web UI. Enter a device Description Enter a user-defined PassPhrase to be used to authenticate the Core to the Central Manager.	Enter Yes; the system will auto-set IP 127.0.0.1 as the All-in-One IP address. Enter the Juniper ATP Appliance Collector Host Name; this identifies the Collector in the Web UI. Enter a device Description Enter a user-defined PassPhrase to be used to authenticate the Core 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 mailto: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" on page 6 for steps.

CLI Help and Keyboard Shortcuts

IN THIS SECTION

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 2: 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 ↑ Ctrl+N or ↓ Ctrl+L or Ctrl+R	Retrieve previous command from CLI history. Retrieve next command from CLI history. Clear the screen or Redisplay the current command line.
Delete	Ctrl+D Ctrl+H Ctrl+K Ctrl+U or Ctrl+W	Delete character. Delete character before cursor (Backspace). Delete all characters from cursor to end of line. Delete all characters or words on line.
Cursor move	Ctrl+A Ctrl+B Ctrl+E Ctrl+F	Move cursor to start of line. Move cursor back a single character. Move cursor to end of line. 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.

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 “core” 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 “collector” 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 “diagnosis” 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 “server” 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 “wizard” in Basic mode. The prompt changes to indicate the mode in parentheses: JATP-Hostname# wizard JATP-Hostname (wizard)# ?	Enter exit to leave wizard mode.

SEE ALSO

All-in-One CLI Commands | 15

All-in-One CLI Commands

IN THIS SECTION

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 20
- "core" on page 23
- "collector" on page 21
- "diagnosis" on page 23
- "exit" on page 24
- "help" on page 26
- "history" on page 27
- "server" on page 34
- "wizard" on page 56

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 24
- "help" on page 26
- "history" on page 27
- "upgrade" on page 55

Core Mode Commands

- "exit" on page 24
- "help" on page 26
- "history" on page 27
- "show (core mode)" on page 50
- "updateimage" on page 55

Server Mode Commands

- "exit" on page 24
- "help" on page 26
- "history" on page 27
- "ifrestart" on page 28
- "ping" on page 29
- "reboot" on page 30
- "restart" on page 31
- "restore" on page 32
- "restore" on page 32
- "set appliance-type (server mode)" on page 41
- "set system-alert (server mode)" on page 46
- "set (server mode)" on page 44
- "shutdown" on page 53
- "shutdown" on page 53
- "traceroute" on page 54

Collector Mode Commands

- "exit" on page 24
- "help" on page 26
- "history" on page 27
- "set honeypot (collector mode)" on page 35
- "set traffic-monitoring (for JATP700 Appliances only) (collector mode)" on page 36
- "set traffic-filter (collector mode)" on page 36
- "set protocols (collector mode)" on page 38

- "set proxy (collector mode)" on page 39
- "show (collector mode)" on page 48

Diagnosis Mode Commands

- "capture-start" on page 20
- "copy" on page 22
- "exit" on page 24
- "gssreport" on page 25
- "help" on page 26
- "history" on page 27
- "set (diagnosis mode)" on page 40
- "setupcheck" on page 47
- "show (diagnosis mode)" on page 51

All-in-One CLI Commands

IN THIS SECTION

capture-start

Table 3: capture-start

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

cm

Table 4: cm

Description	Enters cm (Central Manager) mode. See Also: **basic** [mode];
Product(s) CLI	**All-in-One | Core**

Mode(s)	Basic
Syntax	cm
Parameters	None
Sub-Commands	exit | help | history | upgrade
Example	The following command example enters cm configuration mode: hostname # **cm** hostname (cm)#

collector

Table 5: collector

Description	Enters the Collector configuration mode. See Also: [mode]
Product(s) CLI	**All-in-One | Collector**
Mode(s)	Basic
Syntax	collector
Parameters	None
Sub-Commands	;;;;
Example	The following example enters collector configuration mode: hostname # **collector** hostname (collector)# ?

copy

Table 6: copy

Description	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. The copy traceback command, upon Customer Support's request, copies the traceback files out of the box to a remote location. See Also: [mode];
Product(s) CLI	**All-in-One | Collector | Core-CM | Mac OSX Engine**
Mode(s)	Diagnosis
Syntax	copy capture <scp source_file_name username@destination_host:destination_folder> | traceback {<tab> | ALL} <string URI as user@hostname:path
Parameters	copy capture <scp remote filename_location> copy traceback <ALL | filename> copy traceback <tab> [tab displays all available crash filenames]
Sub-Commands	None
Example	The following example copies the file "Eth1.txt" from the local host to a remote host: hostname (diagnosis)# copy capture Eth1.txt mailto:admin@remotehost.edu:/some/remote/directory

core

Table 7: core

Description	Enters core mode. See Also: **basic** [mode];
Product(s) CLI	**All-in-One | Collector | Core | Mac OS X Detection Engine**
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 8: diagnosis

Description	Enters the Diagnosis configuration and status check mode. See Also: collector [mode], server [mode]
Product(s) CLI	**All-in-One | Collector | Mac OS X Detection Engine**
Mode(s)	Basic
Syntax	diagnosis

Parameters	None
Sub-Commands	;;;;;;;;;
Example	**The following example enters diagnosis configuration and status check mode:** hostname # **diagnosis** hostname (diagnosis)# ?

exit

Table 9: exit

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

gssreport

Table 10: 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: ; [mode]
Product(s) CLI	**All-in-One | Collector | Mac OS X Detection Engine**
Mode(s)	diagnosis
Syntax	gssreport status | submit
Parameters	status - displays the status of the current GSS report. submit - submits a report to Juniper ATP Appliance GSS.
Sub-Commands	None

Example	The following examples display the status of a GSS report submission:
	`    hostname #` **`diagnosis`**
	`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`

help

Table 11: help

Description	Displays information about the CLI help system.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Basic | Core | Collector | Diagnosis | Server
Syntax	help
Parameters	**None**

Example	The following example shows some of the output of the help command. 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 “<cr>” 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: **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? <cr> show firewall whitelist

history

Table 12: history

Description	Displays the current CLI session command line history.

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

ifrestart

Table 13: ifrestart

Description	Restarts the interface driver and services using the interface.
Product(s) CLI	**All-in-One | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server
Syntax	`ifrestart eth0 | eth1`
Parameters	eth0 — Restarts the management network administra interface. eth1 — Restarts the monitoring network interface.

Example	The following example restarts the eth0 interface for the management network. `<FireEye_name># ifrestart eth0`

ping

Table 14: ping

<table>
<tr><td>Description</td><td>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.</td></tr>
<tr><td>Product(s) CLI</td><td>**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**</td></tr>
<tr><td>Mode(s)</td><td>Server</td></tr>
<tr><td>Syntax</td><td>**ping** [**-c** count] [**-h** hops] [string]</td></tr>
<tr><td>Parameters</td><td><table>
<tr><td>**-c**count</td><td>Number of echo requests to send. By default, pings ar continuously until you press Ctrl+C.</td></tr>
<tr><td>**-h**hops</td><td>Number of next hops between pings (default is 1).</td></tr>
<tr><td>string</td><td>IP address, hostname or interface name used to ping device address</td></tr>
</table></td></tr>
</table>

Example	The following example sends three echo requests to the device with the IP Address 10.10.10.1
	<FireEye_name># 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 m`
	`--- 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`

reboot

Table 15: reboot

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

restart

Table 16: restart

Description	Restarts Juniper ATP Appliance services.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server
Syntax	restart [all | behaviorengine | cm | collector | core | correlationengine | database | ntpserver | sshserver | staticengine | webserver]

Parameters	all	Restarts all Juniper ATP Appliance services.
	behaviorengine	Restarts the Behavioral Analysis Engine
	cm	Restarts the Central Manager Web UI service.
	collector	Restarts the Collector service.
	core	Restarts the Core Detection Engine.
	correlationengine	Restarts the Correlation Engine.
	database	Restarts the Database.
	ntpserver	Restarts the NTP server.
	sshserver	Restarts the SSH server.
	staticengine	Restarts the Static Analysis Engine.
	webserver	Restarts the web server.
Example	The following example restarts the Central manager service. `JATP# restart cm`	

restore

Table 17: restore

Description	Restores the system configuration to the factory default settings. This will only reset the password to default temporarily.

<table>
<tr><td>Product(s) CLI</td><td><b>All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine</b></td></tr>
<tr><td>Mode(s)</td><td>server</td></tr>
<tr><td>Syntax</td><td>restore [support | firewall {backup | default} | hostname | network]
Allowlist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the allowist state as rules cannot be saved in that case.</td></tr>
<tr><td>Parameters
<b>NOTE</b>: vCore for AWS does not use the following CLI commands: restore hostname restore network</td><td>
<table>
<tr><td>support</td><td>Restores the default support password setting remote login (set during initial installation per I See also (server)# "set (server mode)" on page 44</td></tr>
<tr><td>firewall {backup | default}</td><td>Restores the firewall settings from either the pr backup, or from the default factory settings.</td></tr>
<tr><td>hostname</td><td>Restores the system’s hostname to the factory hostname.</td></tr>
<tr><td>network</td><td>Restores the IP address and DNS settings to the factory default settings.
<b>WARNING</b>: This command option removes the current IP address and DNS settings, and reloads the default values for these settings.</td></tr>
</table>
</td></tr>
<tr><td>Example</td><td>The following example restores the system.
<code>JATP# <b>restore</b></code>
This next example restores the SSH login “support” password to the default
<code>JATP # <b>restore support password</b></code>
<code>Restore the default support password? (Yes/No)? yes</code>
<code>support password was restored successfully!</code></td></tr>
</table>

server

Table 18: server

Description	Enters the server configuration mode. See Also:
Product(s) CLI	**All-in-One | Collector | Core/CM | Mac Mini Mac OS X**
Mode(s)	Basic
Syntax	server
Sub-Commands	`; ; ; ; ; ; ; ;` Whitelist rules rely on normal service shutdown to be backed up.Powering off a VM directly will lose the allowlist state as rules cannot be saved in that case.

Example	The following example enters server configuration mode:
	`hostname # server`
	`hostname (server) # ?`

set honeypot (collector mode)

Table 19: set honeypot

Description	Enables and disables the SSH-Honeypot feature for a Traffic Collector. 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. There are two parameters that can be set for a honeypot: • Enable/disable a honeypot • Set a Static IP (IP, mask, and gateway) or DHCP of a publicly addressable interface See Also: show honeypot command in
Product(s) CLI	**All-in-One | Collector**
Mode(s)	collector

Syntax	`(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`

Example	The following example enables the SMB parser for lateral detections: `(collector)# set honeypot ssh-honeypot enable address 1.2.3.4 netmask 255.255.0.0 gateway 1.2.3.1` **NOTE**: The static IP configuration does not require configuring DNS. Honeypots do not require a DNS server at this time.

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

Table 20: set traffic-monitoring

Description	Sets the traffic monitoring interface on the JATP700
Product(s) CLI	**All-in-One | Collector**
Mode(s)	collector

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.
	NOTE: After making an interface type change, the system must be rebooted for the change to take effect.

set traffic-filter (collector mode)

Table 21: set traffic-filter

Description	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. See Also:; [show traffic-filter]
Product(s) CLI	**All-in-One | Collector**
Mode(s)	collector

Syntax

```
set traffic-filter {add <rule_name> <domain> <sourceaddress> <destination-
address> <source-port> <destination-port> <protocol> | remove <rule_name>}
```

Parameters

`traffic-filter add`	Adds a traffic filter rule where:
`<RuleString>`	“RuleString” is the name of the rule
`<Dom ainString>`	“DomainString” is the domain to filter out
`<sourc eaddress>`	“source-address” is the source IPv4 address or network (CIDR)
`<destination-address>`	“destination-address” is the destination IPv4 address or network (CIDR)
`<source-port>`	“source-port” is the source port number (0-65535)
`<destinationport>`	“destination-port” is the destination port number
`<protocol>`	(0-65535)“protocol” is the protocol type: either IP, TCP, UDP or HTTP

Example

The following example add a traffic filter rule to the Traffic Collector.

```
JATP-collector02(collector)# set traffic-rule add CustomRule2
headqrts.example.com 10.2.00/16 20.0.0.2 90 120 tcp
```

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).

set protocols (collector mode)

Table 22: set protocols

Description	Enables and disables the HTTP or SMB parser for a Traffic Collector. See Also: show protocols command in
Product(s) CLI	**All-in-One | Collector**
Mode(s)	collector
Syntax	`(collector)# set protocols {http [on|off] | smb [on|off]}`
Example	The following example enables the SMB parser for lateral detections: `hostname (collector) set protocols smb on`

set proxy (collector mode)

Table 23: set proxy

Description	Sets an Inside or Outside data path proxy from collector mode. 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. 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). See Also: ["set proxy" command for management network]; ; **NOTE**: 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-> 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->Firewall page.
Product(s) CLI	**All-in-One | Collector**
Mode(s)	collector
Syntax	set proxy inside {add <proxy IP address> <proxy port> | remove <proxy IP address> <proxy port> set proxy outside {add <proxy IP address> | remove <proxy IP address>

Parameters	inside	Sets the inside proxy IP addresses
	outside	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 add 10.1.1.1 8080`
	The following example sets an outside data path proxy:
	`JATP (collector)# set proxy outside add 10.2.1.1`	

set (diagnosis mode)

Table 24: set

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also:; set (collector mode)
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
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. `JATP# set logging all`	

set appliance-type (server mode)

Table 25: set appliance-type

Description	Change the appliance type at any time. For example, change from All-In-One to Core/CM. Note that if you change the appliance type after the initial installation, all data files related to the current type are lost and you must set up the appliance as you would a fresh box.
Product(s) CLI	All-in-One | Core CM | Collector
Mode(s)	server

Syntax	`jatp:AIO#(server)# set appliance-type core-cm`
Parameters	all-in-one core-cm email-collector traffic-collector

Example	The following example changes the form factor of the appliance from all-in-one (the default) to core-cm:
	`jatp:AIO#(server)# set appliance-type core-cm`
	`This will result in the deletion of all data and configurations not relevant to the new form factor.`
	`Proceed? (Yes/No)?  Yes`

set ip interface (server mode)

Table 26: set ip interface

Description	Sets the management interface (eth0) and/or the alternate-exhaust interface (eth2) for the Juniper ATP Appliance. 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). See Also:;;;
Product(s) CLI	All-in-One | Core CM | Mac Mini OS X Detection Engine

Mode(s)

server

Syntax

```
(server) # set ip interface management <dhcp | address | netmask |
gateway>
```

```
(server) # set ip interface alternate-exhaust <address | netmask |
gateway>
```

Parameters

dhcp	Enables DHCP for the management or alternate-exhaust interface.
address	Sets the static IP address for the management (eth0) or lternate-exhaust (eth2) interface,
netmask	Sets the netmask for the management network or the alternate-exhaust network.
gateway	Sets the Gateway IP address for the management interfac or the optiona alternate-exhaust network.

Example

The following example configures the management interface (eth0) for a Juniper ATP Appliance Core device:

```
JATP (server)# set ip interface management address
10.2.123.18 netmask 255.255.255.0 gateway 10.2.0.1
```

The following example configures the management interface (eth0) using DHCP:

```
JATP (server)# set ip interface management dhcp
```

This example configures the alternate-exhaust interface (eth2) for a Juniper ATP Appliance Core device:

```
JATP (server)# set ip interface alternate-exhaust address 10.2.123.12
netmask 255.255.255.0 gateway 10.2.0.2
```

set (server mode)

Table 27: set

<table>
<tr><td>Description</td><td>Configure the system settings.</td></tr>
<tr><td>Product(s) CLI</td><td>All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine</td></tr>
<tr><td>Mode(s)</td><td>Server, See Also:;</td></tr>
<tr><td>Syntax</td><td><code>set [autoupdate {on | off} | cli timeout secs | clock | cm address | cysupport {enable | disable} localmode {enable | disable}| passphrase string | dns | firewall {all <backup | flush> | whitelist} | hostname string | ip interface {management | alternate-exhaust}| ntpserver | password | proxy {config | enabled | remove} | timezone string | uipassword]</code></td></tr>
<tr><td>Parameters
(Columns below)</td><td>Note: vCore for AWS does not use the following CLI commands:
set ip
set hostname
[Users cannot set static IP address or change the hostname directly on an EC2 AWS instance]
server mode “set proxy” command is a management network proxy tool; for data path Collector proxy configurations, refer to
"set proxy (collector mode)" on page 39</td></tr>
</table>

autoupdate {content | software} {on | off} cli timeout secs clock cm address set cysupport {enable | disable} | {localmode} dns firewall {all <backup | flush> | whitelist <add | delete | flush>} hostname string ip interface {management | alternateexhaust} <dhcp | address | netmask | gateway}	Turn on or off automatic product updates. set autoupdate content on Sets CLI timeout period in seconds (0 indicates no timeout). Sets the current date and time. Sets the IP address of the Central Manager and netmask using the slash notation; example: AAA.BBB.CCC.DD/X Enables remote SSH login “support” account or localmode enable|/ disable. Sets DNS (or enables DHCP for DNS) for the management interface by default if interface is unspecified. Backs up or flushes (clears) all current iptables for a firewall, or adds, deletes or flushes the current iptables allowlist-specific settings for the firewall. The “add” option adds an IP address to the iptables outbound allowlist. # set firewall whitelist add 10.1.1.1 Sets the system’s host name. Sets the IP address, netmask, or default gateway, or enables DHCP for the management or alternate-exhaust interface.
ntpserver passphrase string password	Sets the Network Time Protocol (NTP) server. Sets the device key password; enter a string. Sets a new password for the CLI administrator.
proxy {config <all|http> | enabled <on|off> | remove <all|http>}	Config, enable/disable, or remove “all” proxy configs, or remove an HTTP-specific proxy server. **TIP**: Tip: Config the proxy for “all” protocols first, and then change HTTP proxy as needed.
timezone string	Sets the timezone for the device.

`uipassword`	Sets a new admin password for CM Web UI access.

Example	The following example disables the CLI timeout counter.
	`JATP (server)# set cli timeout 0`
	The following example enables support:
	`JATP (server)# set cysupport enable`

set system-alert (server mode)

Table 28: set system-alert

Description	Configure the traffic threshold and checking interval for the Collector “monitored traffic” health status. 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.
Product(s) CLI	**All-in-One | Core CM**
Mode(s)	Server, See Also:;; show
Syntax	`set system-alert traffic <integer> time <interval>` **NOTE**: Note that both "traffic" and "time" parameters are required in order to set the threshold for both the minimum traffic and time.

<table>
<tr><td>Parameters</td><td><table><tr><td><code>traffic</code></td><td>- the minimum traffic (in KB)</td></tr><tr><td><code>interval</code></td><td>- the checking interval (in minutes)</td></tr></table></td></tr>
<tr><td>Example</td><td><code>JATP (server) # set system-alert traffic 100 time 30</code>
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).
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.
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.</td></tr>
</table>

setupcheck

Table 29: setupcheck

Description	Checks and reports on basic configuration settings and analysis pipeline setup.
Product(s) CLI	**All-in-One | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	diagnosis
Syntax	`setupcheck {all | report | basic | analysis}`

Parameters	`all`	Checks both basic settings and analysis pipelin
	`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 (collector mode)

Table 30: 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	**All-in-One | Collector**
Mode(s)	Collector
Subcommands	`homenet | traffic-filter | proxy | honeypot`
Syntax	show

Parameters	`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

The following example displays the current Collector proxy inside settings:

```
collector02(collector)# show proxy inside
Proxy IPs: 10.1.1.1
```

The following example displays the current traffic filter:

```
collector02 (collector)# show traffic-filter
Name: CustomRule2, Domain: headqtrs.example.com
```

The following example displays the current SMB protocol parser setting:

```
collector02 (collector)# show protocols
```

The following example displays the current honeypot configuration:

```
collector02 (collector)# show honeypot ssh-honeypot
```

show (collector mode)

Table 31: show (collector mode)

Description	Display the currently selected traffic monitoring interface.

Product(s) CLI	**All-in-One | Collector**
Mode(s)	Collector
Syntax	`collector02 (collector)#ow traffic-monitoring-ifc-type` Display the currently selected traffic monitoring interface

show (core mode)

<table>
<tr><td>Description</td><td>Displays the guest image(s) status or allowlist statistics.
See Also:; <b>show (diagnostic mode)</b></td></tr>
<tr><td>Product(s) CLI</td><td><b>See Also: shutdown; show (diagnostic mode)</b></td></tr>
<tr><td>Mode(s)</td><td>Core</td></tr>
<tr><td>Syntax</td><td>show</td></tr>
<tr><td>Parameters</td><td><table>
<tr><td>images</td><td>Displays guest image update and status information.</td></tr>
<tr><td>whitelist</td><td>Displays the name, hit count and the time of last hit of a user configured allowlist.
Note that when a allowlist 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.</td></tr>
<tr><td>alternate-exhaustinterface</td><td>Displays the status of the alternate exhaust interface eth2.</td></tr>
</table></td></tr>
</table>

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 32: show (diagnosis mode)

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also::**show (core mode)**

Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**	
Mode(s)	diagnosis	
Syntax	show	
Parameters	device {collectorstatus | | corestatus | slavecorestatus}	Display connected device statistics for Traffic Collector, CoreCM, or Mac Mini Detection Engine Secondary “backup core.”
	protocol {web | email}	Displays the session counts for network web or email protocols.
	objects	Displays the current number of file objects.
	logging	Displays the currently-configured logging level. See Also:
	log error traceback	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.
	log error last <integer: number of lines to display>	Displays n [1-1000] lines of the contents of the common log file.
		Example: show log error last 12

Example

The following example displays the connected Traffic Collector status.

```
JATP(diagnosis)# show device collectorstatus
<cr>
```

```
 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
```

This example displays the log error traceback

```
JATP(diagnosis)# show log error traceback
<cr>
```

shutdown

Table 33: shutdown

Description	Shuts down the Juniper ATP Appliance server.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server
Syntax	shutdown

Parameters	**None**
Example	The following example performs a shutdown of the current device. `JATP# shutdown`

traceroute

Table 34: traceroute

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

upgrade

Table 35: upgrade

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

updateimage

Table 36: 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	**All-in-One | Core-CM | Mac Mini OS X Detection Engine**

Mode(s)	Core
Syntax	updateimage
Parameters	`built-in` — Updates the guest-image on the detection Engine.

Example	The following example performs a built-in profile update for the Core detection engine.
	`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`

wizard

Table 37: 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	**All-in-One | Core/CM | Collector | Mac Mini Mac OS X**
Mode(s)	Basic
Syntax	`wizard`

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

Configuration Wizard for the All-in-One Server

Table 38: Configuration Wizard for All-in-One Server

Configuration Wizard Prompts	Customer Response Actions
Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)? Note: Only if your DHCP response is `no` ,enter the following information when prompted: 1. IP address (no CIDR format) 2. Netmask 3. Enter a gateway IP address for this management (administrative) interface: 4. Enter primary DNS server IP address. 5. Do you have a secondary DNS Server (Yes/No). 6. Do you want to enter the search domains? 7. Enter the search domain (separate multiple search domains by space): Restart the administrative interface (Yes/No)?	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred. Recommended: Respond with `no`: 1. Enter an IP address 2. Enter a netmask using the form 255.255.255.0. 3. Enter a gateway IP address. 4. Enter the DNS server IP address 5. If `yes` enter the IP address of the secondary DNS server. 6. Enter `yes` if you want DNS lookups to use a specific domain. 7. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com Enter `yes` to restart with the new configuration settings applied.

Enter a valid hostname.	Type a hostname when prompted; do not include the domain; for example: `JuniperATP1`. **NOTE**: Only alphanumeric characters and hyphens (in the middle of the hostname) are allowed.
[OPTIONAL] If the system detects a Secondary Core with an eth2 port, then the alternate CnC exhaust option is displayed: Use alternate-exhaust for the analysis engine exhaust traffic (Yes/No)? Enter IP address for the alternate-exhaust (eth2) interface: Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0) Enter gateway IP Address for the alternateexhaust (eth2) interface: (example:10.6.0.1) Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8) Do you have a secondary DNS server for the alternate-exhaust (eth2) interface? Do you want to enter the search domains for the alternate-exhaust (eth2) interface? **NOTE**: A complete network interface restart can take more than 60 seconds	Refer to “Configuring an Alternate Analysis Engine Interface” in the Juniper ATP Appliance Operator’s Guide for more information. Enter yes to configure an alternate eth2 interface. Enter the IP address for the eth2 interface. Enter the eth2 netmask. Enter the gateway IP address. Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface. Enter yes or no to confirm or deny an eth2 secondary DNS server. Enter yes or no to indicate whether you want to enter search domain.
Regenerate the SSL self-signed certificate (Yes/No)?	Enter `yes` to create a new SSL certificate for the Juniper ATP Appliance Server Web UI.

SEE ALSO

Core/CM Server CLI Commands | 59

Traffic Collector CLI Commands | 137

Core/CM Server CLI Commands

IN THIS SECTION

This chapter describes the commands for 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 64
- "core" on page 64
- "diagnosis" on page 66
- "exit" on page 66
- "help" on page 68
- "history" on page 69

- "server" on page 77
- "wizard" on page 102

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 66
- "help" on page 68
- "history" on page 69
- "upgrade" on page 101

Core Mode Commands

- "exit" on page 66
- "help" on page 68
- "history" on page 69
- "set (core mode)" on page 76
- "show (core mode)" on page 84
- "updateimage" on page 101

Server Mode Commands

- "exit" on page 66
- "help" on page 68
- "history" on page 69
- "ifrestart" on page 70

- "ping" on page 71
- "reboot" on page 72
- "restart" on page 73
- "restore" on page 75
- "set (server mode)" on page 78
- "set appliance-type (server mode)" on page 81
- "server" on page 77
- "show (server mode)" on page 88
- "shutdown" on page 99
- "traceroute" on page 54
- "upgrade" on page 101

Diagnosis Mode Commands

- "capture-start" on page 63
- "copy" on page 65
- "exit" on page 66
- "gssreport" on page 67
- "help" on page 68
- "history" on page 69
- "set (diagnosis mode)" on page 82
- "setupcheck" on page 83
- "show (diagnosis mode)" on page 86

CoreCM CLI Commands

IN THIS SECTION

capture-start

Table 39: capture-start

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

cm

Table 40: cm

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

core

Table 41: core

Description	Enters core mode. See Also: **basic** [mode];
Product(s) CLI	**All-in-One | Collector | Core | Mac OS X Detection Engine**
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)#

copy

Table 42: copy

Description	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. The copy traceback command, upon Customer Support's request, copies the traceback files out of the box to a remote location. See Also:[mode];
Product(s) CLI	**All-in-One | Collector | Core-CM | Mac OSX Engine**
Mode(s)	Diagnosis
Syntax	copy capture <scp source_file_name username@destination_host:destination_folder> | traceback {<tab> | ALL} <string URI as user@hostname:path
Parameters	copy capture <scp remote filename_location> copy traceback <ALL | filename> copy traceback <tab> [tab displays all available crash filenames]
Sub-Commands	None

Example	The following example copies the file "Eth1.txt" from the local host to a remote host: hostname (diagnosis)# copy capture scp captureEth1.txt mailto:admin@remotehost.edu:/some/remote/directory

diagnosis

Table 43: diagnosis

Description	Enters the Diagnosis configuration and status check mode. See Also: collector [mode], server [mode]
Product(s) CLI	**All-in-One | Collector | Mac OS X Detection Engine**
Mode(s)	Basic
Syntax	diagnosis
Parameters	None
Sub-Commands	; ; ; ;;;;;;
Example	The following example enters diagnosis configuration and status check mode: hostname # diagnosis hostname (diagnosis)# ?

exit

Table 44: exit

Description	Ends the CLI session.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**

Mode(s)	Basic | Core | Collector | Diagnosis | Server
Syntax	exit
Parameters	None

Example	The following example ends a command mode or CLI session.
	`JATP# (diagnosis) exit`
	`JATP#`

gssreport

Table 45: 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:;[mode]
Product(s) CLI	**All-in-One | Collector | Mac OS X Detection Engine**
Mode(s)	diagnosis
Syntax	gssreport status | submit
Parameters	status - displays the status of the current GSS report. submit - submits a report to Juniper ATP Appliance GSS.
Sub-Commands	None

Example

The following examples display the status of a GSS report submission:

```
    hostname # diagnosis
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
```

help

Table 46: help

Description	Displays information about the CLI help system.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Basic | Core | Collector | Diagnosis | Server
Syntax	help
Parameters	**None**

Example	The following example shows some of the output of the help command.

```
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 “<cr>” 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:
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?
<cr>
show firewall whitelist
```

history

Table 47: history

Description	Displays the current CLI session command line history.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**

Mode(s)	Basic | Core | Collector | Diagnosis | Server
Syntax	**hi**story
Parameters	None
Example	The following examples returns command line history for the current CLI session. `JATP# (core) history`

ifrestart

Table 48: ifrestart

Description	Restarts the interface driver and services using the interface.
Product(s) CLI	**All-in-One | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server
Syntax	ifrestart eth0 | eth1

Parameters	`eth0          Restarts the management network administra interface.`
	`eth1          Restarts the monitoring network interface.`

Example	The following example restarts the eth0 interface for the management network. `<FireEye_name># ifrestart eth0`

ping

Table 49: ping

<table>
<tr><td>Description</td><td>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.</td></tr>
<tr><td>Product(s) CLI</td><td><b>All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine</b></td></tr>
<tr><td>Mode(s)</td><td>Server</td></tr>
<tr><td>Syntax</td><td><b>ping</b> [<b>-c</b> count] [<b>-h</b> hops] [string]</td></tr>
<tr><td>Parameters</td><td><table>
<tr><td><b>-c</b>count</td><td>Number of echo requests to send. By default, pings ar continuously until you press Ctrl+C.</td></tr>
<tr><td><b>-h</b>hops</td><td>Number of next hops between pings (default is 1).</td></tr>
<tr><td>string</td><td>IP address, hostname or interface name used to ping device address</td></tr>
</table></td></tr>
<tr><td>Example</td><td>The following example sends three echo requests to the device with the IP Address 10.10.10.1

<FireEye_name># ping -c 3 10.10.10.1
<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 m

--- 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></td></tr>
</table>

reboot

Table 50: reboot

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

reset-admin-password

Table 51: reset-admin-password

Description	A sudo user named “recovery” uses this command to reset the admin password. This user will not require any password and can only login on a physical device, not using ssh login.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server
Syntax	recovery
Parameters	exit | help| history | reset-admin-password

Example	The following example resets the admin password. `customer login: recovery` **NOTE**: Since passwords do not sync across devices, you must perform this reset manually on all JATP devices.

restart

Table 52: restart

Description	Restarts Juniper ATP Appliance services.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server
Syntax	restart [all | behaviorengine | cm | collector | core | correlationengine | database | ntpserver | sshserver | staticengine | webserver]

Parameters	all	Restarts all Juniper ATP Appliance services.
	behaviorengine	Restarts the Behavioral Analysis Engine
	cm	Restarts the Central Manager Web UI service.
	collector	Restarts the Collector service.
	core	Restarts the Core Detection Engine.
	correlationengine	Restarts the Correlation Engine.
	database	Restarts the Database.
	ntpserver	Restarts the NTP server.
	sshserver	Restarts the SSH server.
	staticengine	Restarts the Static Analysis Engine.
	webserver	Restarts the web server.

Example

The following example restarts the Central manager service.

```
JATP# restart cm
```

restore

Table 53: restore

<table>
<tr><td>Description</td><td>Restores the system configuration to the factory default settings. This will only reset the password to default temporarily.</td></tr>
<tr><td>Product(s) CLI</td><td><b>All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine</b></td></tr>
<tr><td>Mode(s)</td><td>server</td></tr>
<tr><td>Syntax</td><td>restore [support | firewall {backup | default} | hostname | network]

Allowlist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the allowist state as rules cannot be saved in that case.</td></tr>
<tr><td>Parameters

<b>NOTE</b>: vCore for AWS does not use the following CLI commands: restore hostname restore network</td><td>
<table>
<tr><td>support</td><td>Restores the default support password setting remote login (set during initial installation per I See also (server)# "set (server mode)" on page 78</td></tr>
<tr><td>firewall {backup | default}</td><td>Restores the firewall settings from either the pr backup, or from the default factory settings.</td></tr>
<tr><td>hostname</td><td>Restores the system's hostname to the factory hostname.</td></tr>
<tr><td>network</td><td>Restores the IP address and DNS settings to the factory default settings.

<b>WARNING</b>: This command option removes the current IP address and DNS settings, and reloads the default values for these settings.</td></tr>
</table>
</td></tr>
</table>

Example	The following example restores the system.
	`JATP# restore`
	This next example restores the SSH login “support” password to the default
	`JATP # restore support password`
	`Restore the default support password? (Yes/No)? yes`
	`support password was restored successfully!`

set (core mode)

Table 54: set

Description	Resets the Secondary Core UUID, if the virtual core is cloned.
Product(s) CLI	Core/CM (Virtual Core)
Mode(s)	Core (for Virtual Core configurations)
Syntax	set id
Sub-Commands	None

Example	The following example sets the Virtual Core appliance id:
	`hostname # core`
	`hostname (core) # set id`
	`<cr>`

server

Table 55: server

Description	Enters the server configuration mode.
Product(s) CLI	**All-in-One | Collector | Core/CM | Mac Mini Mac OS X**
Mode(s)	Basic
Syntax	server
Sub-Commands	;;;;;;;;; Whitelist rules rely on normal service shutdown to be backed up.Powering off a VM directly will lose the allowlist state as rules cannot be saved in that case.

Example	The following example enters server configuration mode:
	`hostname # server`
	`hostname (server) # ?`

set system-alert (server mode)

Table 56: set system-alert

Description	Configure the traffic threshold and checking interval for the Collector “monitored traffic” health status. 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.
Product(s) CLI	**All-in-One | Core CM**
Mode(s)	Server, See Also:; **set (collector mode)**; **show**

Syntax	`set system-alert traffic <integer> time <interval>` **NOTE**: Note that both "traffic" and "time" parameters are required in order to set the threshold for both the minimum traffic and time.

Parameters	`traffic - the minimum traffic (in KB)`
	`interval - the checking interval (in minutes)`

Example	`JATP (server) # set system-alert traffic 100 time 30` 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). 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. 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.

set (server mode)

Table 57: set

Description	Configure the system settings.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server, See Also: ; ;

Syntax	`set [autoupdate {on | off} | cli timeout secs | clock | cm address | cysupport {enable | disable} localmode {enable | disable}| passphrase string | dns | firewall {all <backup | flush> | whitelist} | hostname string | ip interface {management | alternate-exhaust}| ntpserver | password | proxy {config | enabled | remove} | timezone string | uipassword]`

Parameters
NOTE: vCore for AWS does not use the following CLI commands:
`set ip`
`set hostname`
[Users cannot set static IP address or change the hostname directly on an EC2 AWS instance]
(See columns below)	

`autoupdate {content | software} {on | off}`
`cli secs`
clock
`cm address`
`set cysupport {enable | disable} | {localmode}`
dns
`firewall {all <backup | flush> | whitelist <add | delete | flush>}`
`hostname string`
`ip interface {management | alternateexhaust} <dhcp | address | netmask | gateway}`
	Turn on or off automatic product updates.
	`set autoupdate content on`
	Sets CLI period in seconds (0 indicates no timeout).
	Sets the current date and time.
	Sets the IP address of the Central Manager and netmask using slash notation; ex: AAA.BBB.CCC.DD/X
	Enables remote SSH login “support” account or localmode enable|/disable.
	Sets DNS (or enables DHCP for DNS) for the management interface by default if interface is unspecified.
	Backs up or flushes (clears) all current iptables for a firewall, or adds, deletes or flushes the current iptables allowlist-specific settings for the firewall.
	The “add” option adds an IP address to the iptables outbound allowlist.
	# set firewall whitelist add 10.1.1.1
	Sets the system’s host name.
	Sets the IP address, netmask, or default gateway, or enables DHCP for the management or alternate-exhaust interface.

`ntpserver`
`passphrase string`
`password`
	Sets the Network Time Protocol (NTP) server.
	Sets the device key password; enter a string.
	Sets a new password for the CLI administrator.

`proxy {config <all|http> | enable <on|off> | remove <all|http>}`	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.

`timezone string`	Sets the timezone for the device.
`uipassword`	Sets a new admin password for CM Web UI access.
Examples	The following example enables a proxy server. `JATP (server)# set proxy enable on`

set appliance-type (server mode)

Table 58: set appliance-type

Description	Change the appliance type at any time. For example, change from All-In-One to Core/CM. Note that if you change the appliance type after the initial installation, all data files related to the current type are lost and you must set up the appliance as you would a fresh box.
Product(s) CLI	All-in-One | Core CM | Collector
Mode(s)	server
Syntax	`jatp:AIO#(server)# set appliance-type core-cm`
Parameters	all-in-one core-cm email-collector traffic-collector

Example	The following example changes the form factor of the appliance from all-in-one (the default) to core-cm:
	`jatp:AIO#(server)# set appliance-type core-cm`
	`This will result in the deletion of all data and configurations not`
	`relevant to the new form factor.`
	`Proceed? (Yes/No)?  Yes`

set (diagnosis mode)

Table 59: set

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also:
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
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# set logging all	

setupcheck

Table 60: setupcheck

Description	Checks and reports on basic configuration settings and analysis pipeline setup.
Product(s) CLI	**All-in-One | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	diagnosis
Syntax	setupcheck {all | report | basic | analysis}

Parameters	`all            Checks both basic settings and analysis pipelin`
	`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 61: show

Description	Displays the guest image(s) status or allowlist statistics. See Also:; **show (diagnostic mode)**
Product(s) CLI	**See Also: shutdown; show (diagnostic mode)**
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 allowlist. Note that when a allowlist 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-exhaustinterface	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)

Description

Sets the logging levels for Juniper ATP Appliance components from diagnosis mode.

See Also:

Product(s) CLI

All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine

Mode(s)

diagnosis

Syntax	show	
Parameters	device {collectorstatus | | corestatus | slavecorestatus}	Display connected device statistics for Traffic Collector, CoreCM, or Mac Mini Detection Engine Secondary “backup core.”
	protocol {web | email}	Displays the session counts for network web or email protocols.
	objects	Displays the current number of file objects.
	logging	Displays the currently-configured logging level. See Also: set traffic-filter (collector mode) logging
	log error traceback	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.
	log error last <integer: number of lines to display>	Displays n [1-1000] lines of the contents of the common log file.
		Example: show log error last 12

Example

The following example displays the connected Traffic Collector status.

```
JATP(diagnosis)# show device collectorstatus
<cr>
```

```
 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
```

This example displays the log error traceback

```
JATP(diagnosis)# show log error traceback
<cr>
```

show (server mode)

Table 62: show

Description	Display configurations and status information.
Product(s)CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server, See Also:

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.
`cysupport`	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 | alternateexhaust]`	Show information about the management (administrative) network interface eth0, or the monitoring interface (eth1), or the alternate-exhaust interface (eth2).
See Also: `show controller`	Show the IP address of the management (administrative) interface eth0.
ip	Results may show both private and public IP addresses if the AWS vCore has a public IP.
`name`	Show the server name.
`ntpserver`	Show the Network Time Protocol (NTP) server settings.
`proxy`	Shows the proxy configuration for the management network. Show system statistics:
See also show (collector mode) for show proxy inside/outside data path	**cpuload** shows average CPU load in the system for running processes in the last 1, 5 and 15 min intervals.

`stats [cpuload | disk | memory]`	`disk` shows the disk space usage in the system. **memory**shows the system memory usage. `show stats cpuload (0.06,0.13,0.13)`
`system-alert`	Shows the current set system-alert settings.

```
set timezone
```

Shows the list of available timezones as displayed below.

```
Africa/Abidjan                   Africa/Accra                     Africa/
Addis_Ababa               Africa/Algiers                   Africa/
Asmara                    Africa/Asmera
Africa/Bamako                    Africa/Bangui                    Africa/
Banjul                    Africa/Bissau                    Africa/
Blantyre                  Africa/Brazzaville
Africa/Bujumbura                 Africa/Cairo                     Africa/
Casablanca                Africa/Ceuta                     Africa/
Conakry                   Africa/Dakar
Africa/Dar_es_Salaam             Africa/Djibouti                  Africa/
Douala                    Africa/El_Aaiun                  Africa/
Freetown                  Africa/Gaborone
Africa/Harare                    Africa/Johannesburg              Africa/
Juba                      Africa/Kampala                   Africa/
Khartoum                  Africa/Kigali
Africa/Kinshasa                  Africa/Lagos                     Africa/
Libreville                Africa/Lome                      Africa/
Luanda                    Africa/Lubumbashi
Africa/Lusaka                    Africa/Malabo                    Africa/
Maputo                    Africa/Maseru                    Africa/
Mbabane                   Africa/Mogadishu
Africa/Monrovia                  Africa/Nairobi                   Africa/
Ndjamena                  Africa/Niamey                    Africa/
Nouakchott                Africa/Ouagadougou
Africa/Porto-Novo                Africa/Sao_Tome                  Africa/
Timbuktu                  Africa/Tripoli                   Africa/
Tunis                     Africa/Windhoek
America/Adak                     America/Anchorage                America/
Anguilla                 America/Antigua                  America/
Araguaina                America/Argentina/Buenos_Aires
America/Argentina/Catamarca      America/Argentina/ComodRivadavia America/
Argentina/Cordoba        America/Argentina/Jujuy          America/
Argentina/La_Rioja       America/Argentina/Mendoza
America/Argentina/Rio_Gallegos   America/Argentina/Salta          America/
Argentina/San_Juan       America/Argentina/San_Luis       America/
Argentina/Tucuman        America/Argentina/Ushuaia
America/Aruba                    America/Asuncion                 America/
Atikokan                 America/Atka                     America/
Bahia                    America/Bahia_Banderas
America/Barbados                 America/Belem                    America/
Belize                   America/Blanc-Sablon             America/
Boa_Vista                America/Bogota
America/Boise                    America/Buenos_Aires             America/
Cambridge_Bay            America/Campo_Grande             America/
```

```
Cancun                   America/Caracas
America/Catamarca                America/Cayenne                  America/
Cayman                   America/Chicago                  America/
Chihuahua                America/Coral_Harbour
America/Cordoba                  America/Costa_Rica               America/
Creston                  America/Cuiaba                   America/
Curacao                  America/Danmarkshavn
America/Dawson                   America/Dawson_Creek             America/
Denver                   America/Detroit                  America/
Dominica                 America/Edmonton
America/Eirunepe                 America/El_Salvador              America/
Ensenada                 America/Fort_Nelson              America/
Fort_Wayne               America/Fortaleza
America/Glace_Bay                America/Godthab                  America/
Goose_Bay                America/Grand_Turk               America/
Grenada                  America/Guadeloupe
America/Guatemala                America/Guayaquil                America/
Guyana                   America/Halifax                  America/
Havana                   America/Hermosillo
America/Indiana/Indianapolis     America/Indiana/Knox             America/
Indiana/Marengo          America/Indiana/Petersburg       America/Indiana/
Tell_City        America/Indiana/Vevay
America/Indiana/Vincennes        America/Indiana/Winamac          America/
Indianapolis             America/Inuvik                   America/
Iqaluit                  America/Jamaica
America/Jujuy                    America/Juneau                   America/
Kentucky/Louisville      America/Kentucky/Monticello      America/
Knox_IN                  America/Kralendijk
America/La_Paz                   America/Lima                     America/
Los_Angeles              America/Louisville               America/
Lower_Princes            America/Maceio
America/Managua                  America/Manaus                   America/
Marigot                  America/Martinique               America/
Matamoros                America/Mazatlan
America/Mendoza                  America/Menominee                America/
Merida                   America/Metlakatla               America/
Mexico_City              America/Miquelon
America/Moncton                  America/Monterrey                America/
Montevideo               America/Montreal                 America/
Montserrat               America/Nassau
America/New_York                 America/Nipigon                  America/
Nome                     America/Noronha                  America/
North_Dakota/Beulah      America/North_Dakota/Center
America/North_Dakota/New_Salem   America/Nuuk                     America/
Ojinaga                  America/Panama                   America/
Pangnirtung              America/Paramaribo
```

```
America/Phoenix                  America/Port-au-Prince           America/
Port_of_Spain            America/Porto_Acre               America/
Porto_Velho              America/Puerto_Rico
America/Punta_Arenas             America/Rainy_River              America/
Rankin_Inlet             America/Recife                   America/
Regina                   America/Resolute
America/Rio_Branco               America/Rosario                  America/
Santa_Isabel             America/Santarem                 America/
Santiago                 America/Santo_Domingo
America/Sao_Paulo                America/Scoresbysund             America/
Shiprock                 America/Sitka                    America/
St_Barthelemy            America/St_Johns
America/St_Kitts                 America/St_Lucia                 America/
St_Thomas                America/St_Vincent               America/
Swift_Current            America/Tegucigalpa
America/Thule                    America/Thunder_Bay              America/
Tijuana                  America/Toronto                  America/
Tortola                  America/Vancouver
America/Virgin                   America/Whitehorse               America/
Winnipeg                 America/Yakutat                  America/
Yellowknife              Antarctica/Casey
Antarctica/Davis                 Antarctica/DumontDUrville
Antarctica/Macquarie             Antarctica/Mawson
Antarctica/McMurdo               Antarctica/Palmer
Antarctica/Rothera               Antarctica/South_Pole
Antarctica/Syowa                 Antarctica/Troll
Antarctica/Vostok                Arctic/Longyearbyen
Asia/Aden                        Asia/Almaty                      Asia/
Amman                       Asia/Anadyr                      Asia/
Aqtau                       Asia/Aqtobe
Asia/Ashgabat                    Asia/Ashkhabad                   Asia/
Atyrau                      Asia/Baghdad                     Asia/
Bahrain                     Asia/Baku
Asia/Bangkok                     Asia/Barnaul                     Asia/
Beirut                      Asia/Bishkek                     Asia/
Brunei                      Asia/Calcutta
Asia/Chita                       Asia/Choibalsan                  Asia/
Chongqing                   Asia/Chungking                   Asia/
Colombo                     Asia/Dacca
Asia/Damascus                    Asia/Dhaka                       Asia/
Dili                        Asia/Dubai                       Asia/
Dushanbe                    Asia/Famagusta
Asia/Gaza                        Asia/Harbin                      Asia/
Hebron                      Asia/Ho_Chi_Minh                 Asia/
Hong_Kong                   Asia/Hovd
Asia/Irkutsk                     Asia/Istanbul                    Asia/
```

```
Jakarta                     Asia/Jayapura                    Asia/
Jerusalem                   Asia/Kabul
Asia/Kamchatka                   Asia/Karachi                     Asia/
Kashgar                     Asia/Kathmandu                   Asia/
Katmandu                    Asia/Khandyga
Asia/Kolkata                     Asia/Krasnoyarsk                 Asia/
Kuala_Lumpur                Asia/Kuching                     Asia/
Kuwait                      Asia/Macao
Asia/Macau                       Asia/Magadan                     Asia/
Makassar                    Asia/Manila                      Asia/
Muscat                      Asia/Nicosia
Asia/Novokuznetsk                Asia/Novosibirsk                 Asia/
Omsk                        Asia/Oral                        Asia/
Phnom_Penh                  Asia/Pontianak
Asia/Pyongyang                   Asia/Qatar                       Asia/
Qostanay                    Asia/Qyzylorda                   Asia/
Rangoon                     Asia/Riyadh
Asia/Saigon                      Asia/Sakhalin                    Asia/
Samarkand                   Asia/Seoul                       Asia/
Shanghai                    Asia/Singapore
Asia/Srednekolymsk               Asia/Taipei                      Asia/
Tashkent                    Asia/Tbilisi                     Asia/
Tehran                      Asia/Tel_Aviv
Asia/Thimbu                      Asia/Thimphu                     Asia/
Tokyo                       Asia/Tomsk                       Asia/
Ujung_Pandang               Asia/Ulaanbaatar
Asia/Ulan_Bator                  Asia/Urumqi                      Asia/Ust-
Nera                    Asia/Vientiane                   Asia/
Vladivostok                 Asia/Yakutsk
Asia/Yangon                      Asia/Yekaterinburg               Asia/
Yerevan                     Atlantic/Azores                  Atlantic/
Bermuda                 Atlantic/Canary
Atlantic/Cape_Verde              Atlantic/Faeroe                  Atlantic/
Faroe                   Atlantic/Jan_Mayen               Atlantic/
Madeira                 Atlantic/Reykjavik
Atlantic/South_Georgia           Atlantic/St_Helena               Atlantic/
Stanley                 Australia/ACT                    Australia/
Adelaide               Australia/Brisbane
Australia/Broken_Hill            Australia/Canberra
Australia/Currie                 Australia/Darwin
Australia/Eucla                  Australia/Hobart
Australia/LHI                    Australia/Lindeman
Australia/Lord_Howe              Australia/Melbourne
Australia/NSW                    Australia/North
Australia/Perth                  Australia/Queensland
Australia/South                  Australia/Sydney
```

```
Australia/Tasmania               Australia/Victoria
Australia/West                   Australia/Yancowinna             Brazil/
Acre                      Brazil/DeNoronha                 Brazil/
East                      Brazil/West
Canada/Atlantic                  Canada/Central                   Canada/
Eastern                   Canada/Mountain                  Canada/
Newfoundland              Canada/Pacific
Canada/Saskatchewan              Canada/Yukon                     Chile/
Continental                Chile/EasterIsland              Etc/
GMT                          Etc/GMT+0
Etc/GMT+1                        Etc/GMT+10                       Etc/GMT
+11                       Etc/GMT+12                       Etc/GMT
+2                        Etc/GMT+3
Etc/GMT+4                        Etc/GMT+5                        Etc/GMT
+6                        Etc/GMT+7                        Etc/GMT
+8                        Etc/GMT+9
Etc/GMT-0                        Etc/GMT-1                        Etc/
GMT-10                       Etc/GMT-11                       Etc/
GMT-12                       Etc/GMT-13
Etc/GMT-14                       Etc/GMT-2                        Etc/
GMT-5                        Etc/GMT-6
```

```
GMT-3                        Etc/GMT-4                        Etc/
```

```
Etc/GMT-7                        Etc/GMT-8                        Etc/
GMT-9                        Etc/GMT0                         Etc/
Greenwich                    Etc/UCT
Etc/UTC                          Etc/Universal                    Etc/
Zulu                         Europe/Amsterdam                 Europe/
Andorra                   Europe/Astrakhan
Europe/Athens                    Europe/Belfast                   Europe/
Belgrade                  Europe/Berlin                    Europe/
Bratislava                Europe/Brussels
Europe/Bucharest                 Europe/Budapest                  Europe/
Busingen                  Europe/Chisinau                  Europe/
Copenhagen                Europe/Dublin
Europe/Gibraltar                 Europe/Guernsey                  Europe/
Helsinki                  Europe/Isle_of_Man               Europe/
Istanbul                  Europe/Jersey
Europe/Kaliningrad               Europe/Kiev                      Europe/
Kirov                     Europe/Lisbon                    Europe/
Ljubljana                 Europe/London
Europe/Luxembourg                Europe/Madrid                    Europe/
Malta                     Europe/Mariehamn                 Europe/
Minsk                     Europe/Monaco
Europe/Moscow                    Europe/Nicosia                   Europe/
Oslo                      Europe/Paris                     Europe/
Podgorica                 Europe/Prague
```

```
Europe/Riga                  Europe/Rome                  Europe/
Samara                Europe/San_Marino            Europe/
Sarajevo              Europe/Saratov
Europe/Simferopol            Europe/Skopje                Europe/
Sofia                 Europe/Stockholm             Europe/
Tallinn               Europe/Tirane
Europe/Tiraspol              Europe/Ulyanovsk             Europe/
Uzhgorod              Europe/Vaduz                 Europe/
Vatican               Europe/Vienna
Europe/Vilnius               Europe/Volgograd             Europe/
Warsaw                Europe/Zagreb                Europe/
Zaporozhye            Europe/Zurich
Indian/Antananarivo          Indian/Chagos                Indian/
Christmas             Indian/Cocos                 Indian/
Comoro                Indian/Kerguelen
Indian/Mahe                  Indian/Maldives              Indian/
Mauritius             Indian/Mayotte               Indian/
Reunion               Mexico/BajaNorte
Mexico/BajaSur               Mexico/General               Pacific/
Apia                 Pacific/Auckland             Pacific/
Bougainville         Pacific/Chatham
Pacific/Chuuk                Pacific/Easter               Pacific/
Efate                Pacific/Enderbury            Pacific/
Fakaofo              Pacific/Fiji
Pacific/Funafuti             Pacific/Galapagos            Pacific/
Gambier              Pacific/Guadalcanal          Pacific/
Guam                 Pacific/Honolulu
Pacific/Johnston             Pacific/Kiritimati           Pacific/
Kosrae               Pacific/Kwajalein            Pacific/
Majuro               Pacific/Marquesas
Pacific/Midway               Pacific/Nauru                Pacific/
Niue                 Pacific/Norfolk              Pacific/
Noumea               Pacific/Pago_Pago
Pacific/Palau                Pacific/Pitcairn             Pacific/
Pohnpei              Pacific/Ponape               Pacific/
Port_Moresby         Pacific/Rarotonga
Pacific/Saipan               Pacific/Samoa                Pacific/
Tahiti               Pacific/Tarawa               Pacific/
Tongatapu            Pacific/Truk
Pacific/Wake                 Pacific/Wallis               Pacific/
Yap                  SystemV/AST4                 SystemV/
AST4ADT              SystemV/CST6
SystemV/CST6CDT              SystemV/EST5                 SystemV/
EST5EDT              SystemV/HST10                SystemV/
MST7                 SystemV/MST7MDT
SystemV/PST8                 SystemV/PST8PDT              SystemV/
```

	`YST9 SystemV/YST9YDT US/`
	`Alaska US/Aleutian`
	`US/Arizona US/Central US/East-`
	`Indiana US/Eastern US/`
	`Hawaii US/Indiana-Starke`
	`US/Michigan US/Mountain US/`
	`Pacific US/Pacific-New US/Samoa`

`timezone {US/Eastern | US/ Central | US/ Mountain`	Show the current timezone; example:
	`set timezone US/Pacific`
	TIP:
	`set timezone <tab> shows options.`

`uptime`	Show how long the system has been running.
`uuid`	Show the system UUID (universally unique ID).
`version`	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 63: shutdown

Description	Shuts down the Juniper ATP Appliance server.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**

Mode(s)	Server
Syntax	**shutdown**
Parameters	None
Example	The following example performs a shutdown of the current device. `JATP# shutdown`

traceroute

Table 64: traceroute

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

upgrade

Table 65: upgrade

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

updateimage

Table 66: 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 a USB drive attached to the Juniper ATP Appliance.
Product(s) CLI	**All-in-One | Core-CM | Mac Mini OS X Detection Engine**
Mode(s)	Core

Syntax	updateimage
Parameters	built-in Updates the guest-image on the detection Engine.

Example	The following example performs a built-in profile update for the Core detection engine.
	`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`

wizard

Table 67: 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	**All-in-One | Core/CM | Collector | Mac Mini Mac OS X**
Mode(s)	Basic
Parameters	wizard
Example	None

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
Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)? **NOTE**: Only if your DHCP response is no,enter the following information when prompted: 1. IP address (no CIDR format) 2. Netmask 3. Enter a gateway IP address for this management (administrative) interface: 4. Enter primary DNS server IP address. 5. Do you have a secondary DNS Server (Yes/No). 6. Do you want to enter the search domains? 7. Enter the search domain (separate multiple search domains by space):	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred. Recommended: Respond with `no`: 1. Enter an IP address 2. Enter a netmask using the form 255.255.255.0. 3. Enter a gateway IP address. 4. Enter the DNS server IP address 5. If `yes`, enter the IP address of the secondary DNS server. 6. Enter `yes` if you want DNS lookups to use a specific domain. 7. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com
Restart the administrative interface (Yes/No)	Enter `yes` to restart with the new configuration settings applied.

Enter a valid hostname.	Type a hostname when prompted; do not include the domain; for example: **juniperatp1** **NOTE**: Only alphanumeric characters and hyphens (in the middle of the hostname) are allowed.
[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)? Enter IP address for the alternate-exhaust (eth2) interface: Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0) Enter gateway IP Address for the alternateexhaust (eth2) interface: (example:10.6.0.1) Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8) Do you have a secondary DNS server for the alternate-exhaust (eth2) interface? Do you want to enter the search domains for the alternate-exhaust (eth2) interface? **NOTE**: A complete network interface restart can take more than 60 seconds	Refer to “Configuring an Alternate Analysis Engine Interface” in the Juniper ATP Appliance Operator’s Guide for more information. Enter yes to configure an alternate eth2 interface. Enter the IP address for the eth2 interface. Enter the eth2 netmask. Enter the gateway IP address. Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface. Enter yes or no to confirm or deny an eth2 secondary DNS server. Enter yes or no to indicate whether you want to enter search domain.
Regenerate the SSL self-signed certificate (Yes/No)?	Enter **yes** to create a new SSL certificate for the Juniper ATP Appliance Server Web UI. If you decline the self-signed certificate by entering no, be prepared to install a certificate authority (CA) certificate.

Enter the following server attributes: Central Manager (CM) IP Address: Device Name: (must be unique) Device Name: (must be unique) Device Key PassPhrase **NOTE**: Remember this passphrase and use it for all distributed devices.	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 a connected Juniper ATP Appliance Collector Device Name; this identifies the Collector in the Web UI. Enter a device Description Enter a user-defined PassPhrase to be used to authenticate the Core to the Central Manager.

SEE ALSO

All-in-One CLI Commands | 15
Traffic Collector CLI Commands | 137

Mac OS X Engine CLI Commands

IN THIS SECTION

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 110
- "diagnosis" on page 111
- "exit" on page 112
- "help" on page 113
- "histroy" on page 114
- "server" on page 119
- "wizard" on page 133

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 112
- "help" on page 113
- "histroy" on page 114
- "show (core mode)" on page 124
- "updateimage" on page 132

Server Mode Commands

- "exit" on page 112
- "help" on page 113
- "histroy" on page 114
- "ifrestart" on page 115
- "ping" on page 116
- "reboot" on page 117
- "restart" on page 117
- "restore" on page 118
- "server" on page 119
- "set (server mode)" on page 120
- "show (server mode)" on page 128
- "shutdown" on page 130
- "traceroute" on page 54

Diagnosis Mode Commands

- "capture-start" on page 109
- "copy" on page 109
- "exit" on page 112
- "gssreport" on page 112
- "help" on page 113
- "histroy" on page 114
- "set (diagnosis mode)" on page 122
- "setupcheck" on page 123
- "show (diagnosis mode)" on page 125

Mac OS X Detection Engine CLI Commands

IN THIS SECTION

capture-start

Table 68: capture-start

Description	Starts packet capture as a means for diagnosing and debugging network traffic and obtaining stats. See Also: "diagnosis" on page 111[mode];"copy" on page 109
Product(s) CLI	**All-in-One | Collector | Core | Mac OS X Detection Engine**
Mode(s)	**Diagnosis**
Syntax	capture-start
Parameters	<IP address> <interface_name>
Sub-Commands	None
Example	The following example starts a packet capture process on interface eth1 for a Traffic Collector with IP address 8.8.8.8: hostname # **diagnosis** hostname (diagnosis)# capture-start 8.8.8.8 eth1 **NOTE**: Note: Address 8.8.8.8 need not be a Juniper ATP Appliance. It is just a host that the capture filters on.

copy

Table 69: 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: [mode];

Product(s) CLI	**All-in-One | Collector | Core | Mac OS X Detection Engine**
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	The following example copies the file "captureEth1.txt" from the local host to a remote host: `hostname (diagnosis)# copy capture scp captureEth1.txt` mailto:admin@remotehost.edu:/some/remote/directory

core

Table 70: core

Description	Enters core mode. See Also: **basic** [mode];
Product(s) CLI	**All-in-One | Collector | Core | Mac OS X Detection Engine**
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 71: diagnosis

Description	Enters the Diagnosis configuration and status check mode. See Also: collector [mode], server [mode]
Product(s) CLI	**All-in-One | Collector | Mac OS X Detection Engine**
Mode(s)	Basic
Syntax	**diagnosis**
Parameters	None
Sub-Commands	;;; ; ; ; ;; ;
Example	The following example enters diagnosis configuration and status check mode: hostname # **diagnosis** hostname (diagnosis)# ?

exit

Table 72: exit

Description	Ends the CLI session.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Basic | Server | Diagnosis
Syntax	exit
Parameters	None

Example	The following example ends a command mode or CLI session.
	`JATP# (diagnosis) exit`
	`JATP#`

gssreport

Table 73: 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:;[mode]
Product(s) CLI	**All-in-One | Collector | Mac OS X Detection Engine**
Mode(s)	diagnosis
Syntax	gssreport status | submit

Parameters	status - displays the status of the current GSS report. submit - submits a report to Juniper ATP Appliance GSS.
Sub-Commands	None

Example	The following examples display the status of a GSS report submission:
	`    hostname # diagnosis`
	`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`

help

Table 74: help

Description	Displays information about the CLI help system.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Basic | Server | Diagnosis
Syntax	help
Parameters	**None**

Example	The following example shows some of the output of the help command. 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 “<cr>” 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: **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? <cr> show firewall whitelist

histroy

Table 75: history

Description	Displays the current CLI session command line history.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**

Mode(s)	Basic | Server | Diagnosis
Syntax	history
Parameters	None
Example	The following examples returns command line history for the current CLI session. `JATP# (core) history`

ifrestart

Table 76: ifrestart

Description	Restarts the interface driver and services using the interface.
Product(s) CLI	**All-in-One | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server
Syntax	ifrestart eth0 | eth1

Parameters	`eth0          Restarts the management network administra`
	`interface.`
	`eth1          Restarts the monitoring network interface.`

Example	The following example restarts the eth0 interface for the management network. `<FireEye_name># ifrestart eth0`

ping

Table 77: 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	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server
Syntax	**ping** [**-c** count] [**-h** hops] [string]
Parameters	**-c**count: Number of echo requests to send. By default, pings ar continuously until you press Ctrl+C. **-h**hops: Number of next hops between pings (default is 1). string: IP address, hostname or interface name used to ping device address

Example	The following example sends three echo requests to the device with the IP Address 10.10.10.1
	<FireEye_name># 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 m`
	`--- 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`

reboot

Table 78: reboot

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

restart

Table 79: restart

Description	Restarts Juniper ATP Appliance services.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server
Syntax	restart [all | behaviorengine | cm | collector | core | correlationengine | database | ntpserver | sshserver | staticengine | webserver]

<table>
<tr><td>Parameters</td><td><table>
<tr><td>all</td><td>Restarts all Juniper ATP Appliance services.</td></tr>
<tr><td>database</td><td>Restarts the Database.</td></tr>
<tr><td>ntpserver</td><td>Restarts the NTP server.</td></tr>
<tr><td>sshserver</td><td>Restarts the SSH server.</td></tr>
</table></td></tr>
<tr><td>Example</td><td>The following example restarts the Central manager service.
JATP# restart cm</td></tr>
</table>

restore

Table 80: restore

Description	Restores the system configuration to the factory default settings. This will only reset the password to default temporarily.
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] Allowlist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the allowist state as rules cannot be saved in that case.

<table>
<tr>
<td>Parameters

<b>NOTE</b>: vCore for AWS does not use the following CLI commands: restore hostname restore network</td>
<td>
<table>
<tr><td>support</td><td>Restores the default support password setting remote login (set during initial installation per l See also (server)# "set (server mode)" on page 120</td></tr>
<tr><td>firewall {backup | default}</td><td>Restores the firewall settings from either the pr backup, or from the default factory settings.</td></tr>
<tr><td>hostname</td><td>Restores the system's hostname to the factory hostname.</td></tr>
<tr><td>network</td><td>Restores the IP address and DNS settings to the factory default settings.

<b>WARNING</b>: This command option removes the current IP address and DNS settings, and reloads the default values for these settings.</td></tr>
</table>
</td>
</tr>
<tr>
<td>Example</td>
<td>The following example restores the system.
<pre>
JATP# restore
</pre>
This next example restores the SSH login “support” password to the default
<pre>
JATP # restore support password
Restore the default support password? (Yes/No)? yes
support password was restored successfully!
</pre>
</td>
</tr>
</table>

server

Table 81: server

Description	Enters the server configuration mode.
Product(s) CLI	**All-in-One | Collector | Core/CM | Mac Mini Mac OS X**

Mode(s)	Basic
Syntax	server
Sub-Commands	`;;;;;;;;;;` Whitelist rules rely on normal service shutdown to be backed up.Powering off a VM directly will lose the allowlist state as rules cannot be saved in that case.

Example	The following example enters server configuration mode:
	`hostname # server`
	`hostname (server) # ?`

set (server mode)

Table 82: set

Description	Configure the system settings.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server, See Also:
Syntax	`set [autoupdate {on | off} | cli timeout secs | clock | cm address | cysupport {enable | disable} localmode {enable | disable}| passphrase string | dns | firewall {all <backup | flush> | whitelist} | hostname string | ip interface {management | alternate-exhaust}| ntpserver | password | proxy {config | enabled | remove} | timezone string | uipassword]`
Parameters (See table below)	

`autoupdate {content | software} {on | off}`	Turn on or off automatic product updates. `set autoupdate content on`
`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 slash notation; ex: AAA.BBB.CCC.DD/X
`set cysupport {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 DNS (or enables DHCP for DNS) for the management interface by default if interface is unspecified.
`firewall {all <backup | flush> | whitelist <add | delete | flush>}`	Backs up or flushes (clears) all current iptables for a firewall, or adds, deletes or flushes the current iptables allowlist-specific settings for the firewall.
NOTE: Whitelist rules rely on normal service shutdown for backup.Powering off a VM directly loses the allowlist state as rules cannot be saved in that case.	The “add” option adds an IP address to the iptables outbound allowlist. # set firewall whitelist add 10.1.1.1
`hostname string`	Sets the system’s host name.
`ip interface {management | alternateexhaust} <dhcp | address | netmask | gateway}`	Sets the IP address, netmask, or default gateway, or enables DHCP for the management or alternate-exhaust interface.
`ntpserver`	Sets the Network Time Protocol (NTP) server.
`password`	Sets a new password for the CLI administrator.

`proxy {config <all|http> | enable <on| off> | remove <all|http>}`	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.
`timezone {US/ Eastern | US/ Central | US/ Mountain`	Show the current timezone; example: set timezone US/Pacific **TIP**: set timezone <tab> shows options.
`uipassword`	Sets a new admin password for CM Web UI access.
Examples	The following example sets an ip address for the device management interface eth0. `JATP# set ip interface 10.1.1.1`

set (diagnosis mode)

Table 83: set

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also:
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	diagnosis
Syntax	set logging

<table>
<tr><td>Parameters</td><td><table>
<tr><td>all</td><td>Sets logging for all Juniper ATP Appliance components.</td></tr>
<tr><td>default</td><td>Sets logging to the default parameters</td></tr>
<tr><td>debug</td><td>Sets logging at the debug level.</td></tr>
<tr><td>info</td><td>Sets logging at the info level.</td></tr>
<tr><td>warning</td><td>Sets logging at the warning level.</td></tr>
<tr><td>error</td><td>Sets logging at the error level.</td></tr>
<tr><td>critical</td><td>Sets logging at the critical level.</td></tr>
</table></td></tr>
<tr><td>Example</td><td>The following example sets the default logging level for all Juniper ATP Appliance components.
<code>JATP# set logging all</code></td></tr>
</table>

setupcheck

Table 84: setupcheck

<table>
<tr><td>Description</td><td>Checks and reports on basic configuration settings and analysis pipeline setup.</td></tr>
<tr><td>Product(s) CLI</td><td><b>All-in-One | Core CM | Mac Mini OS X Detection Engine</b></td></tr>
<tr><td>Mode(s)</td><td>diagnosis</td></tr>
<tr><td>Syntax</td><td><code>setupcheck {all | report | basic | analysis}</code></td></tr>
</table>

Parameters	all	Checks both basic settings and analysis pipelin.
	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 85: show

Description	Displays the guest image(s) status. See Also: ; **show (diagnostic mode)**
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
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 allowlist. Note that when a allowlist 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-exhaustinterface	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 shows how to get the alternate-exhaust interface (eth2) status:
	`JATP(core)# show alternate-exhaust interface`	

show (diagnosis mode)

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also:

Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	diagnosis
Syntax	show

Parameters	device {collectorstatus | | corestatus | slavecorestatus}	Display connected device statistics for Traffic Collector, CoreCM, or Mac Mini Detection Engine Secondary “backup core.” **NOTE**: Not available from the Mac Mini CLI.
	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: set (diagnosis mode) logging
	log error traceback	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.
	log error last <integer: number of lines to display>	Displays n [1-1000] lines of the contents of the common log file.

Example	The following example displays the connected Traffic Collector status.
	`osx-1(server)# show devicetype`
	`Device type: slave_core.`

show (server mode)

Table 86: show

Description	Display configurations and status information.
Product(s)CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server, See Also:
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.
cysupport	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 | alternateexhaust]	(administrative) network interface eth0, or the monitoring interface (eth1), or the alternate-exhaust interface (eth2). See Also: `show controller`
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.
stats [cpuload | disk | memory]	Show system statistics: • `cpuload` shows the average CPU load in the system for running processes in the last 1, 5 and 15 minute intervals. • `disk` shows the disk space usage in the system. • `memory` shows the system memory usage.
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	The following example displays information about the MacOSX cpuload statistics:
	` MacOSX (server)# # show stats cpuload`
	`(0.06, 0.13, 0.13)`
	The following example requests details for the Collector's monitoring interface (eth1):
	`MacOSX(server)# show interface monitoring`

shutdown

Table 87: shutdown

Description	Shuts down the Juniper ATP Appliance server.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server
Syntax	shutdown
Parameters	None

Example	The following example performs a shutdown of the current device. `JATP# shutdown`

traceroute

Table 88: traceroute

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

updateimage

Table 89: 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 a USB drive attached to the Juniper ATP Appliance.
Product(s) CLI	**Mac Mini OS X Detection Engine**
Mode(s)	Core
Syntax	updateimage
Parameters	built-in Updates the guest-image on the Mac OSX Detection “Secondary core.”.

Example	The following example performs a built-in profile update for the Core detection engine.
	`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`

upgrade

Table 90: upgrade

<table>
<tr><td>Description</td><td>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.
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.</td></tr>
<tr><td>Product(s) CLI</td><td><b>Mac Mini OS X Detection Engine</b></td></tr>
<tr><td>Mode(s)</td><td>Core</td></tr>
<tr><td>Syntax</td><td>upgrade</td></tr>
<tr><td>Parameters</td><td><table><tr><td>built-in</td><td>Updates the guest-image on the Mac OSX Detection “secondary core.”.</td></tr></table></td></tr>
<tr><td>Example</td><td>The following example performs a built-in Mac OS X profile update for the Mac Mini-based Secondary core detection engine..
<code>MAC2(core)# upgrade</code></td></tr>
</table>

wizard

Table 91: 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	**All-in-One | Core/CM | Collector | Mac Mini Mac OS X**
Mode(s)	Basic
Parameters	wizard
Example	None
	The following command starts the configuration wizard. `hostname # wizard`

Configuration Wizard Command Prompt Responses

Configuration Wizard Prompts	Customer Response from the Mac Mini

Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)? **NOTE**: Only if your DHCP response is no,enter the following information when prompted: 1. IP address (no CIDR format) 2. Netmask 3. Enter a gateway IP address for this management (administrative) interface: 4. Enter primary DNS server IP address. 5. Do you have a secondary DNS Server (Yes/No). 6. Do you want to enter the search domains? 7. Enter the search domain (separate multiple search domains by space): Restart the administrative interface (Yes/No)?	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred. Recommended: Respond with `no`: 1. Enter an IP address 2. Enter a netmask using the form 255.255.255.0. 3. Enter a gateway IP address. 4. Enter the DNS server IP address 5. If `yes`, enter the IP address of the secondary DNS server. 6. Enter `yes` if you want DNS lookups to use a specific domain. 7. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com Enter `yes` to restart with the new configuration settings applied.
Enter a valid hostname.	Type a hostname when prompted; do not include the domain; for example: `juniperatp1` **NOTE**: Only alphanumeric characters and hyphens (in the middle of the hostname) are allowed.

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

SEE ALSO

All-in-One CLI Commands | 15

Traffic Collector CLI Commands

IN THIS SECTION

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 141
- "diagnosis" on page 143
- "exit" on page 143
- "help" on page 145
- "history" on page 146
- "server" on page 151
- "wizard" on page 172

Collector Mode Commands

- "exit" on page 143
- "help" on page 145
- "history" on page 146
- "set honeypot (collector mode)" on page 154
- "set proxy (collector mode)" on page 153
- "set proxy (collector mode)" on page 153
- "set protocols (collector mode)" on page 156
- "set traffic-filter (collector mode)" on page 160
- "show (collector mode)" on page 163

Diagnosis Mode Commands

- "capture-start" on page 140
- "copy" on page 142
- "exit" on page 143
- "gssreport" on page 144
- "help" on page 145
- "history" on page 146
- "set (diagnosis mode)" on page 155
- "setupcheck" on page 162
- "show (diagnosis mode)" on page 165

Server Mode Commands

- "exit" on page 143

Traffic Collector CLI Commands

IN THIS SECTION

capture-start

Table 92: capture-start

Description	Starts packet capture as a means for diagnosing and debugging network traffic and obtaining stats. See Also: [mode]; [mode];
Product(s) CLI	**All-in-One | Collector**
Mode(s)	Diagnosis
Syntax	capture-start
Parameters	<IP address> <interface_name>

Sub-Commands	None
Example	The following example starts a packet capture process on interface eth1 for a Traffic Collector with IP address 8.8.8.8: hostname # diagnosis hostname (diagnosis)# capture-start 8.8.8.8 eth1 **NOTE**: Note: Address 8.8.8.8 need not be a Juniper ATP Appliance. It is just a host that the capture filters on.

collector

Table 93: collector

Description	Enters the Collector configuration mode. See Also: [mode]
Product(s) CLI	**All-in-One | Collector**
Mode(s)	Basic
Syntax	collector
Parameters	None
Sub-Commands	"exit" on page 143;"help" on page 145; "history" on page 146; "set proxy (collector mode)" on page 153; "show (collector mode)" on page 163

Example	The following example enters collector configuration mode:
	`hostname # collector`
	`hostname (collector)# ?`

copy

Table 94: 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. The `copy traceback` command, upon Customer Support's request, copies the traceback files out of the box to a remote location. See Also: [mode];
Product(s) CLI	**All-in-One | Collector | Core-CM | Mac OSX Engine**
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	The following example copies the file "captureEth1.txt" from the local host to a remote host: `hostname (diagnosis)# copy capture scp captureEth1.txt` mailto:admin@remotehost.edu:/some/remote/directory

diagnosis

Table 95: diagnosis

Description	Enters the Diagnosis configuration and status check mode. See Also: collector [mode], server [mode]
Product(s) CLI	**All-in-One | Collector | Mac OS X Detection Engine**
Mode(s)	Basic
Syntax	diagnosis
Parameters	None
Sub-Commands	"capture-start" on page 140; "copy" on page 142; "exit" on page 143; "gssreport" on page 144; "help" on page 145; "history" on page 146; "set (server mode)" on page 157; "setupcheck" on page 162; "show (diagnosis mode)" on page 165; "show (server mode)" on page 167
Example	The following example enters diagnosis configuration and status check mode: hostname # diagnosis hostname (diagnosis)# ?

exit

Table 96: exit

Description	Ends the CLI session.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Basic | Server | Collector | Diagnosis

Syntax	exit
Parameters	None

Example	The following example ends a command mode or CLI session.
	`JATP# (diagnosis) exit`
	`JATP#`

gssreport

Table 97: 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: ; "diagnosis" on page 143[mode]
Product(s) CLI	**All-in-One | Collector | Mac OS X Detection Engine**
Mode(s)	diagnosis
Syntax	gssreport status | submit
Parameters	status - displays the status of the current GSS report. submit - submits a report to Juniper ATP Appliance GSS.
Sub-Commands	None

Example

The following examples display the status of a GSS report submission:

```
    hostname # diagnosis
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
```

help

Table 98: help

Description	Displays information about the CLI help system.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Basic | Server | Collector | Diagnosis
Syntax	help
Parameters	**None**

Example	The following example shows some of the output of the help command.

```
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 “<cr>” 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:
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?
<cr>
show firewall whitelist
```

history

Table 99: history

Description	Displays the current CLI session command line history.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**

Mode(s)	Basic | Server | Collector | Diagnosis
Syntax	history
Parameters	None
Example	The following examples returns command line history for the current CLI session. JATP# history

ifrestart

Table 100: ifrestart

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

ping

Table 101: ping

<table>
<tr><td>Description</td><td>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.</td></tr>
<tr><td>Product(s) CLI</td><td><b>All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine</b></td></tr>
<tr><td>Mode(s)</td><td>Server</td></tr>
<tr><td>Syntax</td><td><b>ping</b> [<b>-c</b> count] [<b>-h</b> hops] [string]</td></tr>
<tr><td>Parameters</td><td>
<table>
<tr><td><b>-c</b>count</td><td>Number of echo requests to send. By default, pings ar continuously until you press Ctrl+C.</td></tr>
<tr><td><b>-h</b>hops</td><td>Number of next hops between pings (default is 1).</td></tr>
<tr><td>string</td><td>IP address, hostname or interface name used to ping device address</td></tr>
</table>
</td></tr>
<tr><td>Example</td><td>The following example sends three echo requests to the device with the IP Address 10.10.10.1

<FireEye_name># ping -c 3 10.10.10.1
<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 m

--- 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>
</td></tr>
</table>

reboot

Table 102: reboot

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

restart

Table 103: restart

Description	Restarts Juniper ATP Appliance services.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
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	The following example restarts the Central manager service. `JATP# restart cm`	

restore

Table 104: restore

Description	Restores the system configuration to the factory default settings. This will only reset the password to default temporarily.
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] Allowlist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the allowist state as rules cannot be saved in that case.

<table>
<tr><td rowspan="4">Parameters
NOTE: vCore for AWS does not use the following CLI commands: restore hostname restore network</td><td>support</td><td>Restores the default support password setting remote login (set during initial installation per l See also (server)# "set (server mode)" on page 157</td></tr>
<tr><td>firewall {backup | default}</td><td>Restores the firewall settings from either the pr backup, or from the default factory settings.</td></tr>
<tr><td>hostname</td><td>Restores the system’s hostname to the factory hostname.</td></tr>
<tr><td>network</td><td>Restores the IP address and DNS settings to the factory default settings.
WARNING: This command option removes the current IP address and DNS settings, and reloads the default values for these settings.</td></tr>
<tr><td>Example</td><td colspan="2">The following example restores the system.
JATP# **restore**
This next example restores the SSH login “support” password to the default
JATP # **restore support password**
Restore the default support password? (Yes/No)? yes
support password was restored successfully!</td></tr>
</table>

server

Table 105: server

Description	Enters the server configuration mode. See Also:

Product(s) CLI	**All-in-One | Collector | Core/CM | Mac Mini Mac OS X**
Mode(s)	Basic
Syntax	server
Sub-Commands	"exit" on page 143; "help" on page 145; "history" on page 146; "ifrestart" on page 147; "ping" on page 148; "reboot" on page 149;"restore" on page 150; "set (server mode)" on page 157; "show (server mode)" on page 167

Example	The following example enters server configuration mode:
	`hostname # server`
	`hostname (server) # ?`

set proxy (collector mode)

Table 106: set proxy

Description	Sets an Inside or Outside data path proxy from collector mode. 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. 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). See Also: ; **NOTE**: 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-> 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->Firewall page.
Product(s) CLI	**All-in-One | Collector**
Mode(s)	collector

Syntax	`set proxy inside {add <proxy IP address> <proxy port> | remove <proxy IP address> <proxy port>`
	`set proxy outside {add <proxy IP address> | remove <proxy IP address>`

Parameters	<table><tr><td>inside</td><td>Sets the inside proxy IP addresses</td></tr><tr><td>outside</td><td>Sets the outside proxy IP addresses</td></tr><tr><td>add</td><td>Adds a proxy configuration.</td></tr><tr><td>remove</td><td>Removes a proxy configuration.</td></tr></table>

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 inside 10.2.1.1`

set honeypot (collector mode)

Table 107: set honeypot

Description	Enables and disables the SSH-Honeypot feature for a Traffic Collector. 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. There are two parameters that can be set for a honeypot: • Enable/disable a honeypot • Set a Static IP (IP, mask, and gateway) or DHCP of a publicly addressable interface See Also: `show honeypot` command in
Product(s) CLI	All-in-One | Collector

Mode(s)	collector

Syntax	`(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`

Example	The following example enables the SMB parser for lateral detections: `(collector)# set honeypot ssh-honeypot enable address 1.2.3.4 netmask 255.255.0.0 gateway 1.2.3.1` **NOTE**: The static IP configuration does not require configuring DNS. Honeypots do not require a DNS server at this time.

set (diagnosis mode)

Table 108: set

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also: ;
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
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. `JATP# set logging all`	

set protocols (collector mode)

Table 109: set protocols

Description	Enables and disables the HTTP or SMB parser for a Traffic Collector. See Also: `show protocols` command in
Product(s) CLI	**All-in-One | Collector**
Mode(s)	collector
Syntax	(collector)# set protocols {http [on|off] | smb [on|off]}

Example	The following example enables the SMB parser for lateral detections: `hostname (collector) set protocols smb on`

set (server mode)

Table 110: set

Description	Configure the system settings.
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server, See Also:; "set proxy (collector mode)" on page 153
Syntax	set [autoupdate {on | off} | cli timeout secs | clock | cm **address** | cysupport {on | off} | **passphrase string** | dns | firewall {all <backup | flush> | whitelist} | hostname **string** | ip {**interface** | **dhcp** | **address** | **netmask** | **gateway**} | ntpserver | password | proxy {config | enabled | remove} |timezone string | uipassword]
Parameters (See table below)	
`autoupdate {software| content} {on| off}`	Turn on or off the automatic product update feature. `autoupdate {software| content} {on|off}` example: `set autoupdate content on`
`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 cysupport {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>}`	Backs up or flushes (clears) all current iptables for a firewall, or adds, deletes or flushes the current iptables allowlist-specific settings for the firewall. The “add” option adds an IP address to the iptables outbound allowlist. `# set firewall whitelist add 10.1.1.1` Whitelist rules rely on normal service shutdown to be backed up. Powering off a VM directly will lose the allowlist state as rules cannot be saved in that case
`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.

`proxy {config <all|http> | enable <on|off> | remove <all|http>}`	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.
`timezone {US/ Eastern | US/ Central | US/ Mountain`	Show the current timezone; example: set timezone US/Pacific **TIP**: set timezone <tab> shows options.
`uipassword`	Sets a new admin password for CM Web UI access.
Examples	The following example sets an ip address for the device management interface eth0. `JATP# set ip interface 10.1.1.1`

set appliance-type (server mode)

Table 111: set appliance-type

Description	Change the appliance type at any time. For example, change from All-In-One to Core/CM. Note that if you change the appliance type after the initial installation, all data files related to the current type are lost and you must set up the appliance as you would a fresh box.
Product(s) CLI	All-in-One | Core CM | Collector
Mode(s)	server
Syntax	`jatp:AIO#(server)# set appliance-type core-cm`

Parameters	all-in-one core-cm email-collector traffic-collector

Example	The following example changes the form factor of the appliance from all-in-one (the default) to core-cm:
	`jatp:AIO#(server)# set appliance-type core-cm`
	`This will result in the deletion of all data and configurations not relevant to the new form factor.`
	`Proceed? (Yes/No)?  Yes`

set traffic-filter (collector mode)

Table 112: set traffic-filter

Description	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. See Also: ;"show (diagnosis mode)" on page 165 [show traffic-filter]
Product(s) CLI	**All-in-One | Collector**
Mode(s)	collector
Syntac	`set traffic-filter {add <rule_name> <domain> <sourceaddress> <destination-address> <source-port> <destination-port> <protocol> | remove <rule_name>}`

Parameters

`traffic-filter add`	Adds a traffic filter rule where:
`<RuleString>`	“RuleString” is the name of the rule
`<Dom-ainString>`	“DomainString” is the domain to filter out
`<sourc-eaddress>`	“source-address” is the source IPv4 address or network (CIDR)
`<destination-address>`	“destination-address” is the destination IPv4 address or network (CIDR)
`<source-port>`	“source-port” is the source port number (0-65535)
`<destinationport>`	“destination-port” is the destination port number
`<protocol>`	(0-65535)“protocol” is the protocol type: either IP, TCP, UDP or HTTP

Example

The following example add a traffic filter rule to the Traffic Collector.

```
JATP-collector02(collector)# set traffic-rule add CustomRule2
headqrts.example.com 10.2.00/16 20.0.0.2 90 120 tcp
```

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).

## set traffic-monitoring (for JATP700 and JATP400 Appliances) (collector mode)

Table 113: set traffic-monitoring

Description	Sets the traffic monitoring interface on the JATP700 and JATP400.
Product(s) CLI	**All-in-One | Collector**
Mode(s)	collector

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.
	NOTE: After making an interface type change, the system must be rebooted for the change to take effect.

setupcheck

Table 114: setupcheck

Description	Checks and reports on basic configuration settings and analysis pipeline setup.
Product(s) CLI	**All-in-One | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	diagnosis
Syntax	`setupcheck {all | report | basic | analysis}`

Parameters	all	Checks both basic settings and analysis pipelin.
	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 (collector mode)

Table 115: show

Description	Displays the Traffic Collector current traffic filters and the current XFF status (enabled or disabled)
Product(s) CLI	**All-in-One | Collector**
Mode(s)	Collector
Subcommands	`traffic-filter | proxy | honeypot`
Syntax	show

Parameters

`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. See also show proxy:
`honeypot`	Shows the current honeypot configuration. `show honeypot ssh-honeypot`

Example

The following example displays the current Collector proxy inside settings:

```
collector02(collector)# show proxy inside
Proxy IPs: 10.1.1.1
```

The following example displays the current traffic filter:

```
collector02 (collector)# show traffic-filter
Name: CustomRule2, Domain: headqtrs.example.com
```

The following example displays the current SMB protocol parser setting:

```
collector02 (collector)# show protocols
```

show (diagnosis mode)

Table 116: show

Description	Sets the logging levels for Juniper ATP Appliance components from diagnosis mode. See Also:;
Product(s) CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	diagnosis
Syntax	show

Parameters

device {collectorstatus | | corestatus | slavecorestatus}	Display connected device statistics for Traffic Collector, CoreCM, or Mac Mini Detection Engine Secondary “backup core.” **NOTE**: Not available from the Mac Mini CLI.
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: **logging**
log error traceback	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.
log error last <integer: number of lines to display>	Displays n [1-1000] lines of the contents of the common log file. **NOTE**: Not available from the Collector CLI.

NOTE: Example: show log error last 12

Example	The following example displays the connected Traffic Collector status.
	`JATP(diagnosis)# show device collectorstatus`
	`<cr>`
	`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`

show (server mode)

Table 117: show

Description	Display configurations and status information.
Product(s)CLI	**All-in-One | Collector | Core CM | Mac Mini OS X Detection Engine**
Mode(s)	Server, See Also: show (collector mode);
Syntax	`show`
Parameters (See the columns 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.
`cysupport`	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`	Show information about the management (administrative) network interface eth0 and the monitoring interface eth1.
`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.
`name`	Show the server name.
`ntpserver`	Show the Network Time Protocol (NTP) server settings.
`proxy`	Show current proxy configuration.
`uuid`	Show the system UUID (universally unique ID).

`stats [cpuload | disk | memory]`	Show system statistics:
	• `cpuload` shows the average CPU load in the system
	• `disk` shows the disk space usage in the system.
	• `memory` shows the system memory usage.
	`# show stats cpuload`
	`(0.06, 0.13, 0.13)`

`timezone`	Show the current timezone.
`uptime`	Show the last manual upgrade-related information.

`version`	Show Juniper ATP Appliance software and content security versions.

Example	The following example displays information about the All-in-One server device type:
	`All-in-One(server)# show devicetype`
	`Device type: cm, core, web_collector.`

shutdown

Table 118: shutdown

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

traceroute

IN THIS SECTION

Table 119: traceroute

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

wizard

Table 120: 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	**All-in-One | Core/CM | Collector | Mac Mini Mac OS X**
Mode(s)	Basic
Syntax	wizard
Parameters	None
Example	The following command starts the configuration wizard. `hostname #  wizard`

Configuration Wizard Command Prompt Progressions

Table 121: Configuration Wizard

Configuration Wizard Prompts	Customer Response from Collector

Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)? **NOTE**: Only if your DHCP response is `no` ,enter the following information when prompted: 1. IP address (no CIDR format) 2. Netmask 3. Enter a gateway IP address for this management (administrative) interface: 4. Enter primary DNS server IP address. 5. Do you have a secondary DNS Server (Yes/ No). 6. Do you want to enter the search domains? 7. Enter the search domain (separate multiple search domains by space): Restart the administrative interface (Yes/No)?	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred. Recommended: Respond with `no`: 1. Enter an IP address 2. Enter a netmask using the form 255.255.255.0. 3. Enter a gateway IP address. 4. Enter the DNS server IP address 5. If **yes**, enter the IP address of the secondary DNS server. 6. Enter **yes** if you want DNS lookups to use a specific domain. 7. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com Enter `yes` to restart with the new configuration settings applied.
Enter a valid hostname.	Type a hostname when prompted; do not include the domain; for example: `juniperatp1` **NOTE**: Only alphanumeric characters and hyphens (in the middle of the hostname) are allowed.
Regenerate the SSL self-signed certificate (Yes/ No)?	Not applicable to Collector.

Enter the following server attributes: Central Manager (CM) IP Address: Device Name: (must be unique) Device Description Device Key PassPhrase **NOTE**: Remember this passphrase and use it for all distributed devices!	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. Enter the Juniper ATP Appliance Collector Device Name; this identifies the Collector in the Web UI. Enter a device Description Enter the same PassPhrase used to authenticate the Collector to the Central Manager.

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

SEE ALSO

All-in-One CLI Commands | 15

Core/CM Server CLI Commands | 59

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.

Blocklist	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 blocklist, 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

RELATED DOCUMENTATION

All-in-One CLI Commands | 15

Core/CM Server CLI Commands | 59

Mac OS X Engine CLI Commands | 105

Traffic Collector CLI Commands | 137