

Juniper Advanced Threat Prevention Appliance

Core/Central Manager Quick Start Guide

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

408-745-2000

www.juniper.net

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

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

Juniper Advanced Threat Prevention Core/Central Manager Quick Start Guide
Copyright© 2018 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

About the Documentation

Documentation and Release Notes

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

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

Inside This Guide

- JUNIPER ATP APPLIANCE CORE/CM MODEL SPECIFICATIONS
- INSTALLING THE CORE/CM SYSTEM
- INSTALLING THE CORE/CM SYSTEM
- INSTALLING THE JUNIPER ATP APPLIANCE VIRTUAL CORE - OPEN VIRTUAL APPLIANCE (OVA)
- CLUSTERING MULTIPLE CORE+CM (WINDOWS DETECTION) SECONDARY CORES
- CONFIGURING VIRTUAL CORE FOR AWS
- CONFIGURING THE JUNIPER ATP APPLIANCE CORE/CM SYSTEM FROM THE CLI
- ACCESSING THE JUNIPER ATP APPLIANCE CENTRAL MANAGER WEB UI
- MANAGER OF CENTRAL MANAGERS (MCM)
- WHAT TO DO NEXT?

Welcome to the Juniper ATP Appliance Core/Central Manager Quick Start Guide.

Juniper ATP Appliance's continuous traffic monitoring Collectors and multi-platform threat detonation Cores provide actionable malware detection and intelligence, managed by the Juniper ATP Appliance Central Manager. Juniper ATP Appliance inspects network traffic, extracts HTTP web and email objects, then detonates and analyzes potential malware threats using advanced virtualization, big data analysis, and machine learning technologies. Results are reported through the Central Manager Web UI along with auto-mitigation and infection verification options that reach all the way to the enterprise endpoint. SIEM integration is also supported.

Use this guide to perform initial setup of the Juniper ATP Appliance CORE/CM (Central Manager) Server (does not contain an onboard Traffic Collector).

Juniper ATP Appliance Core/CM Model Specifications

The Juniper ATP Appliance APT Defense Solution Core can be deployed in several different ways to best meet the needs of individual networks: As a Hardware Appliance; as a software only ISO image deployed on customer owned hardware; and as a Virtual Machine deployed on VMware ESX servers. Technical specifications per Juniper ATP Appliance Core-CM Server model are provided below.

For hardware specifications and set up instructions, refer to the **Juniper Networks Advanced Threat Prevention 700 Appliance Hardware Guide**.

Firewall & Management Network Interface Connectivity

Connectivity requirements for the Juniper ATP Appliance management interface (eth0) allow for transfer of inspected network and email objects, live malware behavior analysis, intel reporting, and product updates. If the enterprise network firewall uses an outgoing “default allow” rule, this is sufficient. Otherwise, create the following firewall rules:

- SSH port 443 should be open from the Traffic Collector to the Core/CM for traffic inspection and malware behavior analysis as well as consolidate communications and software/security content updates.
- The Core engine connects to a separate Secondary Core Mac Mini OSX Engine or Core+CM Secondary Core using TCP port 22, be sure to open this port when installing a distributed Mac OS X or additional Core+CM (Windows) Secondary Core Engine. All consolidated communications and updates/upgrades take place on eth0. Other ports are reserved in this release.
- If you configure Juniper ATP Appliance Email Collector(s), ports used to access the email server(s) must also be opened. All communications occur across the Juniper ATP Appliance management network via eth0. Other ports are reserved in this release.
- For communication with Juniper ATP Appliance Logging and Update services, the Network Management port (eth0) must be able to communicate to the internet via port 443.

NOTE Primary Core/CM and Secondary Cores/Mac Cores must be on the same network, and allow all ports, with no Port Address (PAT) or Network Address Translation (NAT).

Installing the Core/CM System

To Install the Core/CM Software Images

1. Access and download the raw image from the URL provided by Juniper and convert the raw image to a bootable image. Create a bootable USB drive using this image. Kingston USB flash drives are recommended. There are additional components (sandbox images) required for full functionality. These are downloaded automatically at 12:00am local time after the initial system configuration is complete. (Systems are shipped in PST timezone by default.)
2. Connect the eth0 management network interfaces on the server that will host the Juniper ATP Appliance software and confirm they are active links before beginning the software installation. ISO installation requires at least an active eth0 connection.
3. Insert the USB drive containing the first bootable ISO image to the USB port of the server that will host the Juniper ATP Appliance Core/CM software.
4. At the menu display, select only this option: INSTALL Juniper ATP Appliance SOFTWARE. If you do not see Juniper ATP Appliance Software on the USB drive, select/deselect UEFI boot mode in BIOS.
5. Follow the prompt to remove the USB; the system will reboot itself. This reboot may take up to 20 minutes.
6. After reboot, the Juniper ATP Appliance CLI prompt appears. At the CLI, log in to the Juniper ATP Appliance CLI with the username `admin` and the password `1JATP234`.
7. You will be prompted to insert the 2nd USB drive and to install the second bootable image; answer the prompts:
Do you want to update the guest images automatically [y/n]: n
Do you want to import the guest images from a URL [y/n]: n
Do you want to import the guest images from a USB [y/n]: y
8. The End User License Agreement (EULA) displays; review the displayed EULA and press q to continue.

NOTE When prompted to accept the Juniper ATP Appliance End User License Agreement (EULA), enter `yes`. Configuration cannot continue until the EULA is accepted.
At the prompt, enter a new CLI administrator password. Weak passwords are not accepted. Note that the CLI admin password is maintained separately from the Juniper ATP Appliance Central Manager Web UI

interface. The CM Web UI supports passwords up to 32 characters, and at least 8 characters. Letters (uppercase/lowercase), numbers, and special characters can be used with the exception of double-quotes ("), spaces, or backslash characters (\) in passwords.

9. Prompts for the Configuration Wizard will be displayed. Respond to the Configuration Wizard questions using the following responses outlined in the section [Configuring the Juniper ATP Appliance Core/CM System from the CLI on page 7](#).
10. After completing the CLI Configuration Wizard, install our Juniper ATP Appliance license using the Juniper ATP Appliance Central Manager Web UI Config tab.

When the Configuration Wizard exits to display the CLI, you may use the following commands to view interface configurations and to whitelist an Email Collector (in distributed systems) if one is already installed and configured.

Accessing the Juniper ATP Appliance Central Manager Web UI

To access the Juniper ATP Appliance Central Manager (CM) Web UI, use HTTP/HTTPS; enter the configured Juniper ATP Appliance Server IP address or hostname in any web browser address field, and accept the SSL certificate when prompted. You are required to log into the CM Web UI.

To log into the Central Manager

1. In the Juniper ATP Appliance Login window, enter the default username `admin` and the password `juniper`. The Juniper ATP Appliance Web UI login username and password are separate from the CLI `admin` username and password.
2. When prompted to reset the password, re-enter the password `juniper` as the "old" password, and enter a new password (twice).
3. At login, the Juniper ATP Appliance Central Manager Dashboard is displayed, as shown below. The Dashboard tab includes aggregated malware detection information and provides system status and health information. Additional configurations are made from the Configuration tab. Refer to the Operator's Guide for more information.

Manager of Central Managers (MCM)

The Juniper ATP Appliance Manager of Central Managers (MCM) is a device that provides a Web UI management Web UI for Juniper ATP Appliance customers that deploy multiple Core/Central Managers (CMs) in various geographic locations for which link speed limitations might constrain a single CM deployment. The MCM allows customers with distributed enterprises to centralize their view of detected malware incidents occurring on multiple CMs.

The MCM Platform device type is represented as "mcm" in the Juniper ATP Appliance CLI MCM command mode. The MCM receives incident data from multiple Central Manager (CM) appliances and displays that data in an MCM-mode Web UI.

The MCM Web UI is a subset of the larger Juniper ATP Appliance Central Manager Web UI and includes only the Incidents tab and the Config tab for System Profile configurations, in addition to a device Reset and Logout tab options.

NOTE Refer to the Manager of Central Managers (MCM) User's Guide for information about managing distributed Central Manager devices.

Installing the Juniper ATP Appliance Virtual Core - Open Virtual Appliance (OVA)

Juniper ATP Appliance's extensible deployment options now include a **Virtual Core** (vCore) detection engine product, as an Open Virtual Appliance, or OVA, that runs as a virtual machine. Specifically, a Juniper ATP Appliance OVA-packaged image is available for VMware Hypervisor for vSphere 5.1, 5.5 and 6.0.

An OVF package consists of several files contained in a single directory with an OVF descriptor file that describes the Juniper ATP Appliance virtual machine template and package: metadata for the OVF package, and a Juniper ATP Appliance software image. The directory is distributed as an OVA package (a tar archive file with the OVF directory inside).

vCore Provisioning Requirements

VM vCenter Version Support	Recommended vCore ESXi Hardware	vCore CPUs	vCore Memory
VM vCenter Server Version: 5.5.0 vSphere Client Version: 5.5.0 ESXi version: 5.5.0 and 5.5.1	Processor speed 2.3-3.3 GHz As many physical CORES as virtual CPUs Hyperthreading: either enable or disable	CPU Reservation: Default CPU Limit: Unlimited Hyperthreaded Core Sharing Mode: None (if Hyperthreading is enabled on the ESXi)	Memory Reservation: Default Memory Limit: Unlimited

Model	Number of vCPUs	Memory	Disk Storage
v500M	8	32 GB	Disk 1: 512 G Disk 2: 1 TB
v1G	24	96 GB	Disk 1: 512 G Disk 2: 2 TB

OVA vCore Sizing Options

1. Download the Juniper ATP Appliance OVA file from the location specified by your Juniper ATP Appliance support representative to a desktop system that can access VMware vCenter.
2. Connect to vCenter and click on File>Deploy OVF Template.
3. Browse the Downloads directory and select the OVA file, then click Next to view the OVF Template Details page.
4. Click Next to display and review the End User License Agreement page.
5. Accept the EULA and click Next to view the Name and Location page.
6. The default name for the Virtual Core is Juniper ATP Appliance Virtual Core Appliance. If desired, enter a new name for the Virtual Core.
7. Choose the Data Center on which the vCore will be deployed, then click Next to view the Host/Cluster page.
8. Choose the host/cluster on which the vCore will reside, then click Next to view the Storage page.

9. Choose the destination file storage for the vCore virtual machine files, then click Next to view the Disk Format page. The default is THICK PROVISION LAZY ZEROED which requires 512GB of free space on the storage device. Using Thin disk provisioning to initially save on disk space is also supported. Click Next to view the Network Mapping page.
10. Set up the vCore interface:
 - › Management (Administrative): This interface is used for management and to communicate with the Juniper ATP Appliance Traffic Collectors. Assign the destination network to the port-group that has connectivity to the CM Management Network IP Address.
 - › Click Next to view the Juniper ATP Appliance Properties page.
11. IP Allocation Policy can be configured for DHCP or Static addressing-- Juniper ATP Appliance recommends using STATIC addressing. For DHCP instructions, skip to Step 12. For IP Allocation Policy as Static, perform the following assignments:
 - › IP Address: Assign the Management Network IP Address for the vCore.
 - › Netmask: Assign the netmask for the vCore.
 - › Gateway: Assign the gateway for the vCore.
 - › DNS Address 1: Assign the primary DNS address for the vCore.
 - › DNS Address 2: Assign the secondary DNS address for the vCore.
12. Enter the Search Domain and Hostname for the vCore.
13. Complete the Juniper ATP Appliance vCore Settings:
 - › New Juniper ATP Appliance CLI Admin Password: this is the password for accessing the vCore from the CLI.
 - › Juniper ATP Appliance Central Manager IP Address: If the virtual core is stand-alone (no clustering enabled) or Primary (clustering is enabled), the IP address is 127.0.0.1. If the virtual core is a Secondary, the Central Manager IP address will be the IP address of the Primary.
 - › Juniper ATP Appliance Device Name: Enter a unique device name for the vCore.
 - › Juniper ATP Appliance Device Description: Enter a description for the vCore.
 - › Juniper ATP Appliance Device Key Passphrase: Enter the passphrase for the vCore; it should be identical to the passphrase configured in the Central Manager for the Core/CM. Click Next to view the Ready to Complete page.
14. Do not check the Power-On After Deployment option because you must first (next) modify the CPU and Memory requirements (depending on the vCore model--either 500Mbps, or 1Gbps; refer to [OVA vCore Sizing Options on page 4](#) for sizing information.. It is important to reserve CPU and memory for any virtual deployment.
15. To configure the number of vCPUs and memory:
 - A. Power off the virtual collector.
 - B. Right click on the virtual collector -> Edit Settings
 - C. Select Memory in the hardware tab. Enter the required memory in the Memory Size combination box on the right.
 - D. Select CPU in the hardware tab. Enter the required number of virtual CPUs combination box on the right. Click OK to set.

16. To configure CPU and memory reservation:
 - A. For CPU reservation: Right click on vCore-> Edit settings:
 - B. Select Resources tab, then select CPU.
 - C. Under Reservation, specify the guaranteed CPU allocation for the VM. It can be calculated based on Number of vCPUs *processor speed.
 - D. For Memory Reservation: Right click on vCore -> Edit settings.
 - E. In the Resources tab, select Memory.
 - F. Under Reservation, specify the amount of Memory to reserve for the VM. It should be the same as the memory specified by the Sizing guide.
17. If Hyperthreading is enabled, perform the following selections:
 - A. Right click on the vCore -> Edit settings.
 - B. In the Resources tab, select HT Sharing: None for Advanced CPU.
18. Power on the Virtual Core (vCore).
19. Log into the CLI and use the server mode "show uuid" command to obtain the UUID; send to Juniper to receive your license. Refer to the Operator's Guide for licensing instructions.

To install the Juniper ATP Appliance OVA to a VM

1. Unpack the Juniper ATP Appliance Server and mount it in a 19' rack; follow the instructions included with the rail kit.
2. Connect the management port eth0 to the management network.

NOTE The Juniper ATP Appliance Server eth0 management port is used to access the Command Line Interface (CLI) and browser-based Web UI. It is also the interface through which the Juniper ATP Appliance Server communicates with the Collectors, sends email notifications for detected threats, and executes infection verifications (IVP) at enterprise endpoints, downloads detection intel, and performs logging and SIEM integration.

3. Connect a VGA monitor and USB keyboard to the Juniper ATP Appliance Server to perform the initial configuration. Alternatively, you may perform initial configuration using the serial console (Baud Settings: 115,200 baud, 8N1, no hardware flow control, no XON/XOFF)

Connect the power cable and power up the appliance.

NOTE When an OVA is cloned to create another virtual Secondary Core, the value for column "id" in the Central Manager Appliance table is the same by default. Admins must reset the UUID to make it unique. A new Virtual Core CLI command "set id" is available to reset the UUID on a cloned Virtual Core from the CLI's core mode. Refer to the Juniper ATP Appliance CLI Command Reference to review the Core mode "set id" and "show id" commands. Special characters used in CLI parameters must be enclosed in double quotation marks.

Clustering Multiple Core+CM (Windows Detection) Secondary Cores

The Clustered Core feature allows multiple Core detection engines to run in tandem to support larger networks. Juniper ATP Appliance supports additional secondary Core modules for the detection of both Windows and Mac malware.

The installation procedures for clustering are the same installation procedures set for non-clustered devices.

- The first install (perhaps an existing device currently deployed) will be automatically registered as the Primary whenever a second install takes place.

- A second (or additional) Core+CM or Mac-Mini device automatically joins the Core Cluster on completion of the CLI Setup Wizard. When the configuration wizard asks for the IP address of the CM, enter the IP address of the Core that was first installed.

Installing Clustered Cores

Install the Secondary Core(s) as described below, then configure the CM IP address to point to the existing Primary and set the device key for all Secondary Cores to match that of the Primary.

NOTE Do not change any configuration on the existing Primary device already in use. If all devices are new installations, any device can be the Primary device, and any of the additional devices can be the Secondary Cores. Juniper ATP Appliance supports up to 6 clustered Secondary per Primary installation.

After the installation steps are performed (installation steps are shown below and configuration steps are provided in the section [Configuring the Juniper ATP Appliance Core/CM System from the CLI on page 7](#)), it will take approximately 10 minutes for the Central Manager services to detect the new Secondary Core(s) and initiate detection engine processes on the Secondary Core(s). The Central Manager Web UI will then display the new Secondary Core(s) in the Config->Secondary Cores table from which additional clustered Secondary Core management options can take place.

Allow a few minutes for the Juniper ATP Appliance Server to boot up and be ready to configure, then proceed to [Configuring the Juniper ATP Appliance Core/CM System from the CLI on page 7](#) to set the CM IP address to point to the existing Primary.

Configuring Virtual Core for AWS

Juniper ATP Appliance technology integrates with Amazon Web Services (AWS) by providing Virtual Core images that can be run on the AWS platform. The Virtual Core is provided in an Amazon Machine Images (AMI) format that is launched as an AWS EC2 instance. Refer to the [Juniper ATP Appliance vCore for Amazon AWS Quick Start Guide](#) for more information.

Configuring the Juniper ATP Appliance Core/CM System from the CLI

If you are powering up a Core/CM system in order to change initial configuration settings, you will need to log in as described immediately below.

Logging into the Juniper ATP Appliance Core CLI

1. Log in to the Juniper ATP Appliance CLI with the username `admin` and the password `1JATP234`.
2. When prompted with the query "Do you want to configure the system using the Configuration Wizard (Yes/No)?", enter `yes`.
3. The Juniper ATP Appliance Configuration Wizard steps you through initial configuration of the Juniper ATP Appliance Core/CM system. To exit the CLI, type `exit`. Respond to the Configuration Wizard questions below using the following response options:

Configuration Wizard Prompts	Customer Response Actions
------------------------------	---------------------------

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

<p>[OPTIONAL] If the system detects a Secondary Core with an eth2 port, then the alternate CnC exhaust option is displayed:</p> <p>Use alternate-exhaust for the analysis engine exhaust traffic (Yes/No)?</p> <p>Enter IP address for the alternate-exhaust (eth2) interface:</p> <p>Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0)</p> <p>Enter gateway IP Address for the alternate-exhaust (eth2) interface: (example:10.6.0.1)</p> <p>Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8)</p> <p>Do you have a secondary DNS server for the alternate-exhaust (eth2) interface?</p> <p>Do you want to enter the search domains for the alternate-exhaust (eth2) interface?</p> <p>Note: A complete network interface restart can take more than 60 seconds</p>	<p>Enter yes to configure an alternate eth2 interface.</p> <p>Enter the IP address for the eth2 interface.</p> <p>Enter the eth2 netmask.</p> <p>Enter the gateway IP address.</p> <p>Enter the primary DNS server IP Address for the alternate-exhaust (eth2) interface.</p> <p>Enter yes or no to confirm or deny an eth2 secondary DNS server.</p> <p>Enter yes or no to indicate whether you want to enter search domain.</p>
<p>Regenerate the SSL self-signed certificate (Yes/No)?</p>	<p>Enter yes to create a new SSL certificate for the Juniper ATP Appliance Server Web UI.</p> <p>If you decline the self-signed certificate by entering no, be prepared to install a certificate authority (CA) certificate.</p>
<p>NOTE: The remaining Wizard prompts are specific to Collector or Secondary device configurations.</p>	

Enter the following server attributes:	
Central Manager (CM) IP Address:	Required: Enter the CM external IP address, not the loopback: 127.0.0.1
Device Name: (must be unique)	Enter the Juniper ATP Appliance Collector or Secondary Core Device Name; this identifies the device in the Web UI.
Device Description	
Device Key PassPhrase	Enter a device Description
NOTE: Remember this passphrase and use for all distributed devices!	Enter a user-defined PassPhrase Enter a user-defined pass phrase to be used to authenticate the Collector or Secondary Core to the Central Manager.

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. Please refer to the Operator's Guide for further information regarding the Juniper ATP Appliance Server command line.

Enclose special characters used in CLI parameters in double quotation marks.

What to Do Next?

- Use the Central Manager (CM) Web UI Dashboard and Config pages to confirm traffic monitoring and detection activity. The CM updates security intelligence every 5 minutes, so you may need to wait 5 minutes to see activity at the Web UI.
- For information about configuring a Virtual Core for AWS, refer to the Juniper ATP Appliance vCore for Amazon AWS Quick Start Guide.
- Review the Juniper ATP Appliance Traffic Collectors Quick Start Guide if planning to install additional or remote Web or Email Traffic Collectors.
- Refer to the Juniper ATP Appliance Mac Mini OS X Engine Quick Start Guide for information about installing a Mac Mini Detection Engine.
- Refer to the Juniper ATP Appliance CLI Command Reference for information about Collector CLI commands.
- Refer to the Juniper ATP Appliance Operator's Guide for information about all products and usage.
- Refer to the Juniper ATP Appliance HTTP API Guide for information about accessing and managing Juniper ATP Appliance advanced threat detection using APIs, including processing data, device and software configuration.
- Refer to the Juniper ATP Appliance Manager of Central Managers (MCM) User's Guide for information about managing distributed Central Manager devices.
- Refer to the Juniper ATP Appliance CEF Logging Support for SIEM Integration Guide for information about CEF logging.