



Core/Central Manager Quick Start Guide



Modified: 2018-12-11

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. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the 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.

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 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 the Documentation	ix
	Documentation and Release Notes	ix
	Documentation Conventions	ix
	Documentation Feedback	xi
	Requesting Technical Support	xii
	Self-Help Online Tools and Resources	xii
	Opening a Case with JTAC	xiii
Chapter 1	Core/Central Manager Quick Start Guide	15
	Overview	15
	Juniper ATP Appliance Core/CM Model Specifications	16
	Firewall & Management Network Interface Connectivity	16
	Installing the Core/CM System	17
	To Install the Core/CM Software Images	17
	Accessing the Juniper ATP Appliance Central Manager Web UI	18
	FIPS Mode Overview	19
	Enable FIPS Mode	19
	Reset Passwords and Keys	21
	Manager of Central Managers (MCM)	22
	Installing the JATP Appliance Virtual Core OVA	22
	vCore Provisioning Requirements and Sizing Options	23
	Install the JATP OVA to a VM	23
	To install the JATP Appliance OVA to a VM	26
	Clustering Multiple Core+CM (Windows Detection) Secondary Cores	26
	Installing Clustered Cores	27
	Configuring Virtual Core for AWS	27
	Configuring the Juniper ATP Appliance Core/CM System from the CLI	28
	Logging into the Juniper ATP Appliance Core CLI	28
	Changing the Appliance Type	30
	What to Do Next?	32

List of Figures

Chapter 1	Core/Central Manager Quick Start Guide	15
	Figure 1: Available Appliance Types, CLI appliance-type Command	31

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	x
	Table 2: Text and Syntax Conventions	x
Chapter 1	Core/Central Manager Quick Start Guide	15
	Table 3: Provisioning Requirements	23
	Table 4: Sizing Options	23

About the Documentation

- Documentation and Release Notes on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xii

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 <https://www.juniper.net/documentation/>.

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 <https://www.juniper.net/books>.

Documentation Conventions

Table 1 on page x defines notice icons used in this guide.

Table 1: Notice Icons







Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page x defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

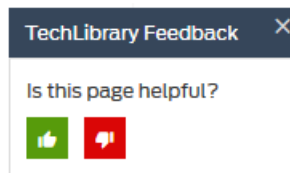
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

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 <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://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 <https://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 <https://www.juniper.net/support/requesting-support.html>.

CHAPTER 1

Core/Central Manager Quick Start Guide

- [Overview on page 15](#)
- [Juniper ATP Appliance Core/CM Model Specifications on page 16](#)
- [Installing the Core/CM System on page 17](#)
- [FIPS Mode Overview on page 19](#)
- [Manager of Central Managers \(MCM\) on page 22](#)
- [Installing the JATP Appliance Virtual Core OVA on page 22](#)
- [Clustering Multiple Core+CM \(Windows Detection\) Secondary Cores on page 26](#)
- [Configuring Virtual Core for AWS on page 27](#)
- [Configuring the Juniper ATP Appliance Core/CM System from the CLI on page 28](#)
- [Changing the Appliance Type on page 30](#)
- [What to Do Next? on page 32](#)

Overview

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

Juniper ATP Appliance's continuous traffic monitoring Collectors and multiplatform 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).

Related Documentation

- [Juniper ATP Appliance Core/CM Model Specifications on page 16](#)
- [Installing the Core/CM System on page 17](#)

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 Appliance Hardware Guide** for your hardware model.

- [Firewall & Management Network Interface Connectivity on page 16](#)

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).

- See Also**
- [Installing the Core/CM System on page 17](#)

Installing the Core/CM System

- [To Install the Core/CM Software Images on page 17](#)
- [Accessing the Juniper ATP Appliance Central Manager Web UI on page 18](#)

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 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
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*.
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.



NOTE: Starting in release 5.0.3, FIPS mode is supported. FIPS mode requires stronger passwords and keys than non-FIPS mode. See [“FIPS Mode Overview” on page 19](#) for details.

- See Also**
- [Manager of Central Managers \(MCM\) on page 22](#)
 - [Changing the Appliance Type on page 30](#)

FIPS Mode Overview

- [Enable FIPS Mode on page 19](#)
- [Reset Passwords and Keys on page 21](#)

Enable FIPS Mode

Federal Information Processing Standards (FIPS) are standards provided by the United States Federal government for the purpose of secure interoperability among computing systems. These standards include encryption and common codes for various types of information, such as emergencies in certain geographic locations.

Starting in release 5.0.3, JATP provides FIPS support, allowing JATP to operate in FIPS 140-2 level 1 compliant mode. From this release onward, JATP can operate in either FIPS or non-FIPS mode.

FIPS mode is enabled or disabled using the CLI. Before you enable FIPS mode, there are several points you should be aware of.

- In clustered deployments, all systems must either be in FIPS mode or not in FIPS mode. This is due to differences in how the device keys are calculated between modes. The same restriction applies for MCM configurations.
- Before enabling FIPS mode, please ensure that the Core/CM, secondary cores, collectors, and other JATP appliances have been successfully upgraded to release 5.0.3 or higher. Enabling FIPS mode will prevent non-FIPS appliances from communicating with, and upgrading from, the Core/CM appliance.
- FIPS mode requires stronger encryption for passwords and keys than non-FIPS mode. Please note the following requirements:
 - Password length (both CLI and UI) must be between 10 to 20 characters long. Passwords cannot use common insecure entries as part of the password, such as “password” or “123456.” Passwords do not have any character uppercase, lowercase, or symbol requirements.
 - User-provided UI private keys must be RSA, 2048 bits or higher.
 - User-provided UI certificates cannot use the following certificate signature hash algorithms: md2, mdc2, ripemd, md4, md5
 - When FIPS mode is enabled, PKCS#12 bundles uploaded to the JATP Core/CM require strong encryption. PKCS#12 bundles with weak encryption cannot be

decrypted and the keypair will not be applied to the UI. Use PBE-SHA1-3DES for the keypbe and certpbe arguments when creating PKCS#12 bundles with the 'openssl pkcs12' command. If the encryption is too weak, you may see the following error message: "Couldn't process SSL Certificate: Error: Failed to extract private key from PKCS#12 bundle."



NOTE: If the above requirements are not met, when you run the command to enable FIPS, the output will indicate the issues you must correct.



WARNING: For existing deployed appliances, you may be prompted to reset the UI and CLI passwords when putting the appliance into FIPS mode. This is because stored passwords are hashed, and it cannot be determined whether or not those passwords meet FIPS requirements.

Enable FIPS mode using the CLI in server mode as follows:



NOTE: If the current password does not meet the FIPS requirements stated above, you must change it before enabling FIPS mode.

Use the **set fips** command with following options to enable and disable FIPS:

```
eng-dhcp (server)# set fips
```

Available options are:

level —Select FIPS 140-2 security level

off —Disable FIPS 140-2 settings

Level 1 is only valid entry at this time. For example, turn FIPS on with the following command:

```
eng-dhcp (server)# set fips level 1
```



NOTE: If all requirements are met and the command is successful, you are prompted to reboot the appliance. FIPS mode settings are applied after the reboot.

Turn FIPS off with the following command:

```
eng-dhcp (server)# set fips off
```

View FIPS settings with the following command:

```
eng-dhcp (server)# show fips
```

View FIPS issues with the following command:

```
eng-dhcp (diagnosis)# show fips errors
```

Reset Passwords and Keys

To reset your passwords and keys (in preparation for enabling FIPS mode or for any other reason):

Enter the **reset** command in server mode:

```
eng-dhcp(server)# reset
```

options are:

ui —Reset all UI settings and remove non-default UI users

passwords —Reset default CLI and UI passwords

keys —Regenerate internal keys and certificates

all —Reset passwords and keys

For example, reset passwords and keys with the following command:

```
eng-dhcp(server)# reset all
```

Example Output:

```
Update passphrases and default accounts ...
Enter the current password of CLI admin:
Enter the new password of CLI admin:
Retype the new password of CLI admin:
Password changed successfully!
Enter the new password of the Central Manager UI account:
Retype the new password of the Central Manager UI account:
Password changed successfully!
Enter new devicekey: securephrase3
Recreating internal keys/certificates (1/4) ...
Recreating internal keys/certificates (2/4) ...
Recreating internal keys/certificates (3/4) ...
Regenerate the SSL self-signed certificate? (Yes/No)? Yes
SSL Self-signed certificate re-generated successfully!
Recreating internal keys/certificates (4/4) ...
This will remove all UI configurations and UI users, except for the default
admin user. All settings, including software/content update, RADIUS, SAML and
GSS settings will be reset to the default settings.
Proceed? (Yes/No)? Yes
----Restarting all services----
```



NOTE: The following prompts from the output above are only applicable for the Core/CM or All-in-one appliance. They are not shown for collectors and secondary cores.

Enter the new password of the Central Manager UI account:

Retype the new password of the Central Manager UI account: Password changed successfully!

This will remove all user configurations and UI users, except for the default admin user.

Proceed? (Yes/No)? Yes

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.

Related Documentation

- [Configuring the Juniper ATP Appliance Core/CM System from the CLI on page 28](#)
- [Clustering Multiple Core+CM \(Windows Detection\) Secondary Cores on page 26](#)

Installing the JATP Appliance Virtual Core OVA

Juniper's Advanced Threat Prevention extensible deployment options include a Virtual Core (vCore) detection engine product as an Open Virtual Appliance, or OVA, that runs as a virtual machine. Specifically, an OVA-packaged image is available for VMware Hypervisor for vSphere 6.5, 6.0, 5.5, and 5.0.

The 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).

Juniper generates an .ovf and a .vmdk file for every JATP build. Download both the OVF and the VMDK into the same directory. Then, from the vSphere client, click on File -> Deploy OVF Template. Choose the .ovf file and then complete the deployment of the ovf wizard. The configuration wizard prompts for collector/core properties such as IP address, hostname, device key. Log in to the CLI and configure each setting.

- [vCore Provisioning Requirements and Sizing Options on page 23](#)
- [Install the JATP OVA to a VM on page 23](#)
- [To install the JATP Appliance OVA to a VM on page 26](#)

vCore Provisioning Requirements and Sizing Options

Table 3: Provisioning Requirements

VM vCenter Version Support	Recommended vCore ESXi Hardware	vCore CPUs	vCore Memory
VM vCenter Server Versions: 6.5, 6.0, 5.5, and 5.0	Processor speed 2.3-3.3 GHz	CPU Reservation: Default	Memory Reservation: Default
vSphere Client Versions: 6.5, 6.0, 5.5, and 5.0	As many physical CORES as virtual CPUs	CPU Limit: Unlimited	Memory Limit: Unlimited
ESXi version: 5.5.1, and 5.5	Hyperthreading: either enable or disable	Hyperthreaded Core Sharing Mode: None (if Hyperthreading is enabled on the ESXi)	

Table 4: Sizing Options

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

Install the JATP OVA to a VM

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 ["Install the JATP OVA to a VM" on page 23](#) 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 JATP 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 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 on page 27](#)

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.



NOTE: If multiple cores are deployed, only a single license is required. That license only needs to be deployed on the primary core.

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*), 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* to set the CM IP address to point to the existing Primary.



NOTE: In clustered deployments, all systems must be either be in FIPS mode or not in FIPS mode. This is due to differences in how the device keys are calculated between modes. See [“FIPS Mode Overview” on page 19](#) for details.

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 *vCore for AWS Quick Start Guide* for more information.

- Related Documentation**
- [Installing the JATP Appliance Virtual Core OVA on page 22](#)

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 on page 28](#)

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
Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)?	We strongly discourage the use of DHCP addressing because it changes dynamically. A static IP address is preferred.
Note: Only if your DHCP response is no, enter the following information when prompted:	Recommended: Respond with no:
a. Enter a gateway IP address and netmask for this management (administrative) interface:	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 primary DNS server IP address	b. Enter the primary DNS IP address
c. Do you have a secondary DNS Server (Yes/No).	c. If yes, enter the IP address of the secondary DNS server.
d. Do you want to enter the search domains?	d. Enter yes if you want DNS lookups to use a specific domain.
e. Enter the search domain (separate multiple search domains by space):	e. 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 unique hostname when prompted; do not include the domain; for example: juniperatp1

<p>[OPTIONAL]</p> <p>If the system detects a Secondary Core with an eth2 port, then the alternate CnC exhaust option is displayed:</p> <p>Use alternate-exhaust for the analysis engine exhaust traffic (Yes/ No)?</p> <p>Enter IP address for the alternateexhaust (eth2) interface:</p> <p>Enter netmask for the alternateexhaust (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>	
<p>Enter the following server attributes: Central Manager (CM) IP Address:</p> <p>Device Name: (must be unique)</p> <p>Device Description</p> <p>Device Key PassPhrase</p> <p>NOTE: NOTE: Remember this passphrase and use for all distributed devices!</p>	<p>Required: Enter the CM external IP address, not the loopback: 127.0.0.1</p> <p>Enter the Juniper ATP Appliance Collector or Secondary Core Device Name; this identifies the device in the Web UI.</p> <p>Enter a device Description</p> <p>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.</p>

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.

See Also • [Manager of Central Managers \(MCM\) on page 22](#)

Changing the Appliance Type

In release version 5.0.4, a single ISO is provided for all appliance types (All-In-One, Email Collector, Traffic Collector, Core/Central Manager). If you don't change the form factor during the installation, all appliances initially boot-up as an All-In-One appliance. You can keep this type or change the type by selecting a different type in the wizard screen that appears following the EULA, after boot-up. See the hardware installation guide for details.

In addition to changing the appliance type after the initial installation, you can change the appliance type at any time using a new CLI command introduced in version 5.0.4 for both JATP700 and JATP400.



WARNING: If you change the appliance type after the initial installation, all data files related to the current type are lost.



NOTE: After you change the appliance type, you must configure the device for the new type as you would any new installation. Follow the installation procedure in the documentation that corresponds to the new appliance type, including setting the passphrase and following the configuration wizard prompts. There is no limit to how many times you can change the appliance type.

To change the appliance type using the CLI, enter the following command while in server mode. (Note that the current appliance type is displayed at the prompt. In this case, the type is "AIO," which is All-In-One.):

```
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
```

The appliance types available from the **set appliance-type** command are listed below and displayed in the following CLI screen:

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



NOTE: When an Email Collector or Traffic Collector is converted to an All In One or Core/CM, you must obtain and apply a new license created for that device identified by its UUID. This is because, after the conversion, the device still uses the existing license, which it obtained and validated from the Core it was connected to previously. Refer to [Setting the Juniper ATP Appliance License Key](#) in the Operator's Guide for instructions on applying a new license.

Figure 1: Available Appliance Types, CLI appliance-type Command

```
*****
*      Juniper Networks Advanced Threat Prevention Appliance      *
*                                                                  *
*****

Welcome admin. It is now Fri Jul 27 11:53:50 PDT 2018
[jatp:AIO# server
Entering the server configuration mode...
[jatp:AIO#(server)# set appliance-type
    all-in-one           All-In-One
    core-cm              Core/Central Manager
    email-collector      Email Collector
    traffic-collector    Traffic Collector

jatp:AIO#(server)# set appliance-type █
```

As mentioned previously, if you change the appliance type after the initial installation, all data files related to the current type are lost. Here are examples of the information that is lost when the appliance type is changed.

- **Core/CM**—If Core/CM is removed from the current appliance type, that will result in the deletion of the following data: all user configurations such as notifications (alert and SIEM settings), system profiles (roles, zones, users, SAML, systems, GSS, collectors and other settings), environmental settings (email and firewall mitigation settings, asset value, identity, splunk configuration and other environmental settings), all file samples, analysis results, events and incidents.
- **Traffic Collector**—If Traffic Collector is removed from the current appliance type, that will result in the deletion of the following data: the data path proxy, traffic rules and all other items configured through the collector CLI.
- **Email Collector**—If Email Collector is removed from the current appliance type, that will result in the deletion of collector related information. Also note that the Email Collector will stop receiving emails.
- **All-In-One**—If All-In-One is removed from the current appliance type, that will result in the following:
 - If you convert from All-In-One to Traffic Collector, then all items mentioned in the Core/CM section above will be removed.

- If you convert from All-In-One to Core/CM, then all settings mentioned in the Traffic Collector section above will be removed.
- If you convert from All-In-One to Email Collector, then all settings mentioned in both the Core/CM and Traffic Collector sections above will be removed.



NOTE: If you are using MCM or Secondary Core and want to change the appliance type to one of the choices available from the “set appliance-type” CLI command, you must first do the following:

- Convert the MCM system back to a Core/CM system by running the **set mcm remove** command from the **cm** menu.
- Convert from a Secondary Core system to a Core system by resetting the CM IP address to 127.0.0.1 and running the **set cm 127.0.0.1** command from the **server** menu.

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.