



Traffic Collector 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.

Traffic Collector 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	Traffic Collector Quick Start Guide	15
	Overview	15
	Firewall & Management Network Interface Connectivity	17
	Installing the Juniper ATP Appliance Collector Open Virtual Appliance (OVA)	17
	Virtual Collector Deployment Options	18
	Provisioning Requirements and Sizing Options	18
	OVA Deployment vSwitch Setup	19
	Install the JATP OVA to a VM	19
	To install the JATP Appliance OVA to a VM	21
	Configuring Juniper ATP Appliance Web Traffic Collection	22
	Setting the same Device Key Passphrase on all Juniper ATP Appliance Devices	23
	Verifying Configurations and Traffic from the CLI	24
	Accessing the Juniper ATP Appliance Central Manager Web UI	24
	Setting SSH Honeypot Detection	25
	Verifying Traffic Collection from the Web UI	26
	Verifying Collector Activity from the Central Manager Web UI	26
	Changing the Appliance Type	28
	What to Do Next?	30

List of Figures

Chapter 1	Traffic Collector Quick Start Guide	15
	Figure 1: DISTRIBUTED TRAFFIC COLLECTOR(S) EXTEND THREAT VISIBILITY	16
	Figure 2: Both the vSwitch and the port-group are in promiscuous mode	17
	Figure 3: Central Manager Web and Email Traffic Collector(s) Configurations . . .	27
	Figure 4: Available Appliance Types, CLI appliance-type Command	29

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	x
	Table 2: Text and Syntax Conventions	x
Chapter 1	Traffic Collector Quick Start Guide	15
	Table 3: Provisioning Requirements	18
	Table 4: Sizing Options	19
	Table 5: Verify CLI Commands	24

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>

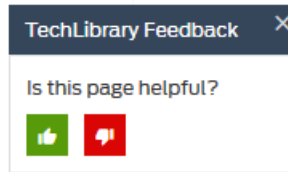
Table 2: Text and Syntax Conventions (continued)

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

Traffic Collector Quick Start Guide

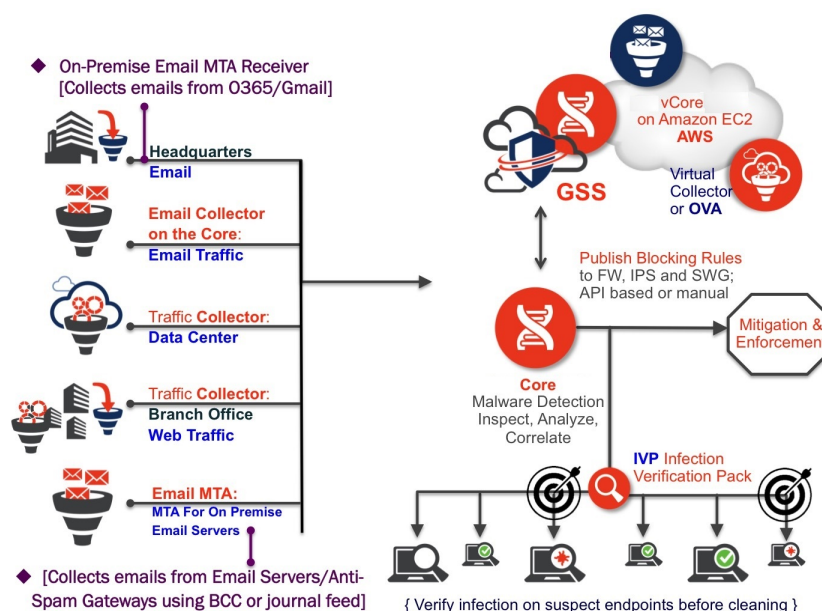
- [Overview on page 15](#)
- [Installing the Juniper ATP Appliance Collector Open Virtual Appliance \(OVA\) on page 17](#)
- [Configuring Juniper ATP Appliance Web Traffic Collection on page 22](#)
- [Setting the same Device Key Passphrase on all Juniper ATP Appliance Devices on page 23](#)
- [Verifying Configurations and Traffic from the CLI on page 24](#)
- [Accessing the Juniper ATP Appliance Central Manager Web UI on page 24](#)
- [Setting SSH Honeypot Detection on page 25](#)
- [Verifying Traffic Collection from the Web UI on page 26](#)
- [Changing the Appliance Type on page 28](#)
- [What to Do Next? on page 30](#)

Overview

Welcome to the Juniper ATP Appliance Traffic Collectors Quick Start Guide.

When linked logically to the Core, the Juniper ATP Appliance Traffic Collectors continuously monitor and inspect all network traffic for malware objects; extracting and sending objects to the Core for Windows or Mac OS X object analysis and detection. Juniper ATP Appliance Web/ Email Collectors efficiently separate traffic monitoring and inspection from behavioral analysis, multi-platform detonation and context reasoning.

Figure 1: DISTRIBUTED TRAFFIC COLLECTOR(S) EXTEND THREAT VISIBILITY



All detected threats and breaches are analyzed by the detonation and intelligence engines within the Juniper ATP Appliance Core, then aggregated and reported in real-time to the Juniper ATP Appliance Central Manager Web UI. In the Web UI, all threats are detailed with corresponding context-specific mitigation options.

Use this guide to install a Juniper ATP Appliance Traffic Collector and to configure its logical connection to a network switch TAP port and a Juniper ATP Appliance Core/CM or All-in-One Server.

- For hardware specifications and set up instructions, refer to the Juniper Networks Advanced Threat Prevention 700 Appliance Hardware Guide.
- For information about installing the Small Form Factor Collector ISO to a Mac Mini, refer to *Installing the Small Form Factor Collector ISO to a Mac Mini*.
- To configure an inside outside data path SPAN-traffic proxy, or management network proxy, refer to the *CLI Command Reference Guide*.



NOTE: This document assumes you have already installed and configured the Juniper ATP Appliance Core/Central Manager or All-in-One Server. Refer to the respective Quick Start Guides for combined and separate Core/Central Manager Server(s), All-in-One, and/or Mac OS X installations.

Firewall & Management Network Interface Connectivity

Connectivity requirements for the Juniper ATP Appliance management interface (eth0) allow for transfer of inspected network objects, live malware behavior analysis, intelligence 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 Collector to the Core/CM or All-in-One (for traffic inspection and malware behavior analysis).

IMPORTANT: 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).



NOTE: All GSS communications for security and content auto-updates are handled by the Core/ CM or All-in-One system.

Related Documentation

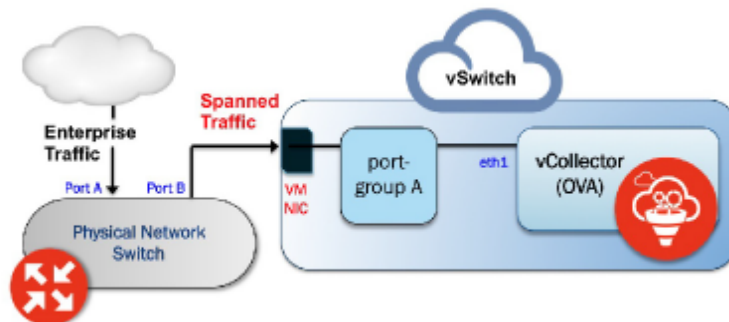
- [Installing the Juniper ATP Appliance Collector Open Virtual Appliance \(OVA\) on page 17](#)
- [Configuring Juniper ATP Appliance Web Traffic Collection on page 22](#)

Installing the Juniper ATP Appliance Collector Open Virtual Appliance (OVA)

Juniper ATP Appliance's extensible deployment options include a Virtual Collector (vCollector) product, as an Open Virtual Appliance, or OVA, that runs in virtual machines. Specifically, a Juniper ATP Appliance OVA-packaged image is available for VMware Hypervisor for vSphere 6.5, 6.0, 5.5 and 5.0. Virtual Collector models supporting 25 Mbps, 100 Mbps, 500 Mbps and a 1.0 Gbps are available.

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).

Figure 2: Both the vSwitch and the port-group are in promiscuous mode



RECOMMENDATION: Juniper advises use of a dedicated physical NIC assigned to the vCollector for best collection results.

- [Virtual Collector Deployment Options on page 18](#)
- [Install the JATP OVA to a VM on page 19](#)
- [To install the JATP Appliance OVA to a VM on page 21](#)

Virtual Collector Deployment Options

Two types of vCollector deployments are supported for a network switch SPAN/TAP:

1. Traffic that is spanned to a vCollector from a physical switch. In this case, traffic is spanned from portA to portB. ESXi containing the Juniper ATP Appliance vCollector OVA is connected to portB. This deployment scenario is shown in the figure above.
2. Traffic from a virtual machine that is on the same vSwitch as the vCollector. In this deployment scenario, because the vSwitch containing the vCollector is in promiscuous mode, by default all port-groups created will also be in promiscuous mode. Therefore, 2 port groups are recommended wherein port-groupA (vCollector) in promiscuous mode is associated with the vCollector, and port-groupB (vTraffic) represents traffic that is not in promiscuous mode.



NOTE: Traffic from a virtual machine that is not on the same vSwitch as the vCollector is not supported. Also, a dedicated NIC adapter is required for the vCollector deployment; attach the NIC to a virtual switch in promiscuous mode (to collect all traffic). If a vSwitch is in promiscuous mode, by default all port-groups are put in promiscuous mode and that means other regular VMs are also receiving unnecessary traffic. A workaround for that is to create a different port-group for the other VMs and configure without promiscuous mode.

- [Provisioning Requirements and Sizing Options on page 18](#)
- [OVA Deployment vSwitch Setup on page 19](#)

Provisioning Requirements and Sizing Options

Table 3: Provisioning Requirements

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

Table 4: Sizing Options

Model	Performance	Number of vCPUs	Memory	Disk Storage
vC-v50M	50 Mbps	1	1.5GB	16 GB
vC--v100M	100 Mbps	2	4 GB	16 GB
vC--v500M	500 Mbps	4	16 GB	512 GB
vC--v1G	1 Gbps	8	32 GB	512 GB
vC-v2.5G	2.5 Gbps	24	64 GB	512 GB

OVA Deployment vSwitch Setup

1. Identify the physical network adapter from which the spanned traffic is received, then create a new VMware Virtual Switch and associate it with the physical network adapter.
2. Click on Virtual Switch Properties. On the Ports tab, select vSwitch and click on the Edit button.
3. Select the Security tab and change Promiscuous Mode to accept, then click OK. Click OK again to exit.
4. Create a new port-group "vtraffic" in the Virtual Switch. This new port-group will be assigned to your vCollector later. See **vSwitch** Tip below for information about troubleshooting this setup.

Install the JATP OVA to a VM

1. Download the Juniper ATP Appliance OVA file from the location specified.
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 Collector is Juniper ATP Appliance Virtual Collector Appliance. If desired, enter a new name for the Virtual Collector.

7. Choose the Data Center on which the vCollector will be deployed, then click Next to view the Host/Cluster page.
8. Choose the host/cluster on which the vCollector will reside, then click Next to view the Storage page.
9. Choose the destination file storage for the vCollector virtual machine files, then click Next to view the Disk Format page. The default is THIN 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 two vCollector interfaces:
 - Management (Administrative): This interface is used to communicate with the Juniper ATP Appliance Central Manager (CM). Assign the destination network to the port-group that has connectivity to the CM Management Network IP Address.
 - Monitoring: This interface is used to inspect and collect network traffic. Assign the destination network to a port-group that is receiving mirrored traffic; this is the port-group "vtraffic" configured in the requirements section above. Click Next to view the Juniper ATP Appliance Properties page.
11. IP Allocation Policy can be configured for DHCP or Static addressing-- Juniper 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 Virtual Collector; it should be in the same subnet as the management IP address for the Juniper ATP Appliance Central Manager.
 - Netmask: Assign the netmask for the Virtual Collector.
 - Gateway: Assign the gateway for the Virtual Collector.
 - DNS Address 1: Assign the primary DNS address for the Virtual Collector.
 - DNS Address 2: Assign the secondary DNS address for the Virtual Collector.
12. Enter the Search Domain and Hostname for the Virtual Collector.
13. Complete the Juniper ATP Appliance vCollector Settings:
 - New Juniper ATP Appliance CLI Admin Password: this is the password for accessing the Virtual Collector from the CLI.
 - Juniper ATP Appliance Central Manager IP Address: Enter the management network IP Address configured for the Central Manager. This IP Address should be reachable by the Virtual Collector Management IP Address.
 - Juniper ATP Appliance Device Name: Enter a unique device name for the Virtual Collector.

- Juniper ATP Appliance Device Description: Enter a description for the Virtual Collector.
 - Juniper ATP Appliance Device Key Passphrase: Enter the passphrase for the Virtual Collector; 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 Virtual Collector model--either 100Mbps, 500Mbps, or 1Gbps; refer to [“OVA Deployment vSwitch Setup” on page 19](#) 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 vCollector-> 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 vCollector -> 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 virtual collector -> Edit settings.
 - b. In the Resources tab, select HT Sharing: None for Advanced CPU.
 18. Power on the Virtual Collector.

To install the JATP Appliance OVA to a VM

1. Obtain requisite login information from your sales representative, then download the Juniper ATP Appliance ISO file [JATP.iso] and the Juniper ATP Appliance Collector image file [img.zip] to your Linux system's local directory.
2. Start a terminal session then plug in the first USB drive (Kingston USB flash drives are recommended) to the Linux system and identify its drive ID (ls /dev/sd*).

3. Use the Linux “dd” utility to write the local ISO content to the first USB flash drive; we refer to drive “sdb” in our example below but your drive ID will likely be different:

```
dd if=JATP.iso of=/dev/sdb
```



NOTE: It is very important that you take note of the drive ID and install the ISO only to that correct USB drive or the dd utility will overwrite all data on the drive selected.

4. OPTIONAL: To view status, use the pv utility [you may need to install the pv utility first]; for example: `dd if=JATP.iso | pv | dd of=/dev/sdb`
5. When the ISO is fully copied to the bootable USB drive, remove USB drive1 and insert USB drive2.
6. Copy the zipped Collector image file `img.zip` to the 2nd USB drive:
7. You are now ready to install the Collector ISO from the bootable USB drive. The ISO will unzip and install the Collector image file.



NOTE: There are Windows Utilities that are also available for creating bootable USB drives from the ISO image.

Related Documentation

- [Changing the Appliance Type on page 28](#)

Configuring Juniper ATP Appliance Web Traffic Collection

When powered up, the Juniper ATP Appliance Collector performs its boot process and then displays a CLI login prompt. Use the following procedure to configure the Juniper ATP Appliance Server using the CLI command line and Configuration Wizard.



NOTE: FOR OVA DEPLOYMENTS: this configuration process is optional and can be skipped because these settings are addressed during OVA deployment to the VM vSwitch.



TIP: Integration requirements for the Email Collector: Microsoft Exchange 2010+

To Configure the Collector

1. In the Login window, enter the default username **admin** and the password **juniper**.



NOTE: 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).

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.

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 Config tab. The main Juniper ATP Appliance CM Web UI tabs are described below.

The Traffic Collector will now automatically “call home” to the Central Manager to announce it is online and active.

Wait ~5 minutes and confirm Collector connectivity from the Juniper ATP Appliance Web UI, as described further below.

When the Configuration Wizard exits to display the CLI, you may use the commands listed in *Verifying Configurations and Traffic from the CLI* to view interface configurations and to whitelist an Email Collector (in distributed systems) if one is already installed and configured. Special characters used in CLI parameters must be enclosed in double quotation marks.

4. To exit the CLI, type **exit**. Be sure to confirm Collector activity from the Juniper ATP Appliance Central Manager Web UI (below).

```
JATP (collector)# exit
```

Related Documentation

- [Setting the same Device Key Passphrase on all Juniper ATP Appliance Devices on page 23](#)
- [Verifying Configurations and Traffic from the CLI on page 24](#)

Setting the same Device Key Passphrase on all Juniper ATP Appliance Devices

The same device key must be set on all Juniper ATP Appliances in your network, no matter how remote the distributed devices may be. To set a device key passphrase, SSH into the device, login, and use the following CLI commands:

```
JATP (server)# set passphrase <strongPassphraseHash>
```

```
JATP (server)# show device key
```

Most characters are valid for the passphrase, except for the following cases:

- Passphrases including white spaces must be put inside quotations “”.
- Passphrases including the character \ must be put inside quotations “”.
- If the passphrase includes the “ character, the “ character itself needs to be escaped.



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

Verifying Configurations and Traffic from the CLI

To verify interface configurations, use the following CLI commands. Refer also to the Juniper ATP Appliance CLI Command Reference for more information and to set traffic-filter and x-forwarded-for configurations:

Table 5: Verify CLI Commands

CLI Mode & Command	Purpose
JATP (diagnosis)# setupcheck all	Run a check of all system components
JATP (server)# show interface	Verify interface connectivity and status
JATP (server)# show ip <interface>	Verify traffic [example: show ip eth1]
JATP (server)# ping x.x.x.x	Ping connected devices.
JATP (diagnosis)# capture-start <IP address> <interface>	Starts packet capture as a means for diagnosing and debugging network traffic and obtaining stats (not part of the Collector traffic capture engine).

NOTE: Be sure to refer to the Juniper ATP Appliance CLI Command Reference for more information. Special characters used in CLI parameters must be enclosed in double quotation marks.

Accessing the Juniper ATP Appliance Central Manager Web UI

To access the Juniper ATP Appliance Central Manager (CM) Web UI, use HTTP/HTTPS and enter the configured Juniper ATP Appliance CM IP address or hostname in a web browser address field, then accept the SSL certificate when prompted. Login is required

To Log in to the Central Manager Web UI

- The Juniper ATP Appliance CM Dashboard views (Operations | Research | System | Collectors [Web | Email]) provide in-context and aggregated malware detection information as well as system status and health statistics.

Use the Config>Web Collectors and Config>Email Collectors tab to verify that a new Collector is calling the Central Manager (CM) Web UI, and is online and actively inspecting and collecting traffic. Instructions are provided in the next section and the Operator's Guide.

Related Documentation

- [Verifying Configurations and Traffic from the CLI on page 24](#)

Setting SSH Honeypot Detection

A honeypot deployed within a customer enterprise network can be used to detect network activity generated by malware attempting to infect or attack other machines in a local area network. Attempted SSH login honeypots are used to supplement detection of lateral spread events. A honeypot can be deployed on a customer Traffic Collector from which event information is sent to the Juniper ATP Appliance Core for processing. Customers can place a honeypot on any local network they desire.

A malicious actor attempting to perform brute force SSH entry, or execute targeted SSH access to a "root" account, will also be detected by the Juniper ATP Appliance SSH Honeypot feature.

Results of SSH Honeypot detections are displayed on the Central Manager Web UI Incidents page, and included in generated Reports.

Data sent to the Juniper ATP Appliance GSS for honeypot detection events include "Threat Target" and a detailing of all attempted "SSH sessions" (including username and password) with timestamps.



NOTE: A Juniper ATP Appliance Enterprise License is required for SSH Honeypot lateral Detection configurations.

A honeypots can operate on a Juniper ATP Appliance All-in-One system or on a Traffic Collector-only device, as long as the host has enough physical interfaces. Each honeypot uses two interfaces, one externally-facing interface for internet/intranet traffic and one for internal host-to-guest communication. This means that each honeypot will use the eth3 interface for all outbound traffic.



TIP: Note that eth3 is not necessarily the fourth interface on a device. On a Collector-only device with three interfaces, the interfaces are named eth0, eth1, and eth3. A collector with four interfaces uses eth0, eth1, eth2, and eth3 naming. If a Collector has less than three interfaces, then the honeypot feature cannot be enabled. An All-in-One device requires at least four interfaces for

the honeypot feature, because the 3rd interface is already reserved as the analysis exhaust interface.

SSH Honeypot is configured from the Juniper ATP Appliance device CLI. There are two parameters that can be set for a honeypot:

- Enable/disable the honeypot
- Provide a Static IP (IP, mask, and gateway) or DHCP of the publicly addressable interface



NOTE: The static IP configuration does not require configuring DNS; at this time, honeypots do not require a DNS server.

For more information:

- Refer to the CLI Command Reference for usage of the SSH Honeypot commands.
- Refer to the Operator's Guide for information about honeypots and lateral detections.

Verifying Traffic Collection from the Web UI

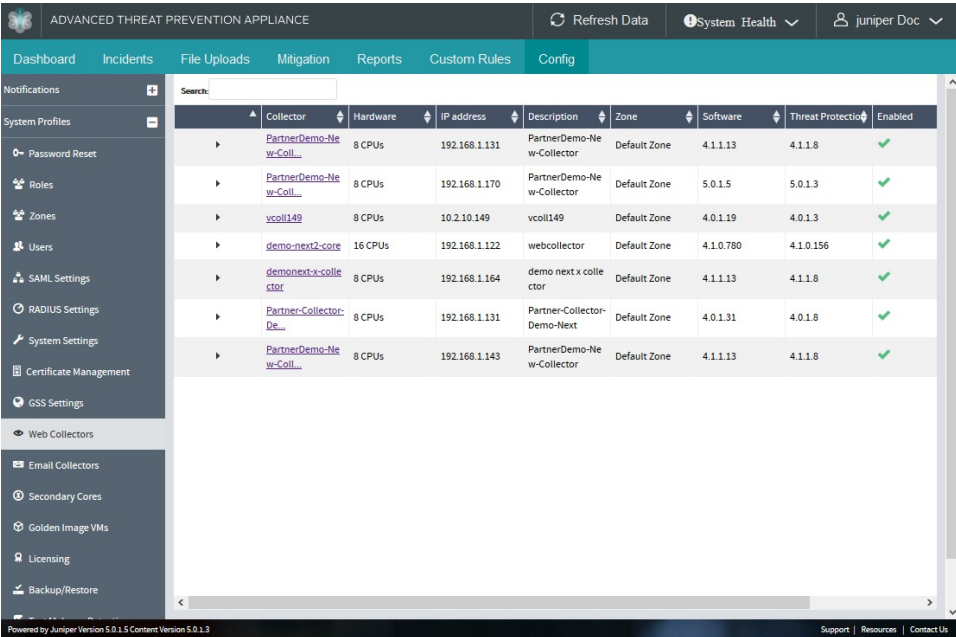
Verify that configured Collectors are calling the Central Manager (CM) Web UI and are online and actively collecting traffic. Use the CLI to show interface and packet statistics; see *Verifying Configurations and Traffic from the CLI*.

- [Verifying Collector Activity from the Central Manager Web UI on page 26](#)

Verifying Collector Activity from the Central Manager Web UI

- Select Config>System Settings> Web Collectors or Config>System Settings> Email Collectors from the Central Manager Web UI to confirm Collector(s) connectivity.

Figure 3: Central Manager Web and Email Traffic Collector(s) Configurations



The screenshot shows the Juniper ATP Appliance Central Manager Web UI. The top navigation bar includes 'Dashboard', 'Incidents', 'File Uploads', 'Mitigation', 'Reports', 'Custom Rules', and 'Config'. The left sidebar contains various system settings like 'Password Reset', 'Roles', 'Zones', 'Users', 'SAML Settings', 'RADIUS Settings', 'System Settings', 'Certificate Management', 'GSS Settings', 'Web Collectors', 'Email Collectors', 'Secondary Cores', 'Golden Image VMs', 'Licensing', and 'Backup/Restore'. The main content area displays a table of Web Collectors with the following columns: Collector, Hardware, IP address, Description, Zone, Software, Threat Protection, and Enabled.

Collector	Hardware	IP address	Description	Zone	Software	Threat Protection	Enabled
PartnerDemo-Ne w-Coll...	8 CPUs	192.168.1.131	PartnerDemo-Ne w-Collector	Default Zone	4.1.1.13	4.1.1.8	✓
PartnerDemo-Ne w-Coll...	8 CPUs	192.168.1.170	PartnerDemo-Ne w-Collector	Default Zone	5.0.1.5	5.0.1.3	✓
vcoll149	8 CPUs	10.2.10.149	vcoll149	Default Zone	4.0.1.19	4.0.1.3	✓
demo-next2-core	16 CPUs	192.168.1.122	webcollector	Default Zone	4.1.0.780	4.1.0.156	✓
demonext-x-colle ctor	8 CPUs	192.168.1.164	demonext x colle ctor	Default Zone	4.1.1.13	4.1.1.8	✓
Partner-Collector- De...	8 CPUs	192.168.1.131	Partner-Collector- Demo-Next	Default Zone	4.0.1.31	4.0.1.8	✓
PartnerDemo-Ne w-Coll...	8 CPUs	192.168.1.143	PartnerDemo-Ne w-Collector	Default Zone	4.1.1.13	4.1.1.8	✓

- Once the Collectors have called home to the CM, further configuration options and modifications are available from the Configuration Web UI pages.



NOTE: The Central Manager updates Collector activity and intelligence every 5 minutes.

To verify traffic collection from the CLI, refer to Verifying Configurations and Traffic from the CLI in this guide.

Be sure to refer to the CLI Command Reference for all command details syntax and usage. Be sure to refer to the CLI Command Reference for all command details syntax and usage.



TIP: A Web Collector or Secondary Core will be shown as down if it has not reported to the Juniper ATP Appliance Central Manager for longer than 25 minutes (in other words, 5 reporting cycles).

RECOMMENDATION: Juniper recommends you clear the system database after becoming familiar with incidents and kill chain flows. If you are running a trial version, clear the database and remove sample incidents and events before putting the system into full production.



NOTE: Refer to the Operator's Guide for information about using the Incidents page and the interactive Dashboard views.

**Related
Documentation**

- [Setting SSH Honeypot Detection on page 25](#)

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 4: 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?

- Navigate to the Config tab and select System Profiles> Licensing from the left panel; upload your license key (obtained from your sales representative).



NOTE: SMB Lateral Detection and SSH Honeypot Detection require an Enterprise License.

- 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. Refer to the Operator's Guide for more detailed information.
- For Email Traffic Collector deployments, refer to the Operator's Guide for information about deploying Collectors in MSSP Tenant Zones, configuring Email Detection Enhancements, Email Threat Quarantine options, and Email Journaling.
- Refer to the Core/CM Quick Start Guide or All-in-One Quick Start Guide for more information about installing and managing distributed Collectors.
- Refer to the Mac Mini OS X Quick Start Guide for information about installing a Mac Mini Detection Engine.
- Refer to the CLI Command Reference for information about Collector CLI commands.
- Refer to the Operator's Guide for information about all products and usage.

- Refer to the API Guide for information about accessing and managing advanced threat detection using APIs, including processing data, device and software configuration.
- Refer to the CEF Logging Support for SIEM Integration Guide for information about CEF logging.

