

# Juniper Advanced Threat Prevention Appliance

## All-in-One Quick Start Guide

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

408-745-2000

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

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

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

Juniper Advanced Threat Prevention All-in-One 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

- EXTENSIBLE INSTALLATIONS
- CONFIGURING THE JUNIPER ATP APPLIANCE ALL-IN-ONE SYSTEM
- SETTING THE SAME DEVICE KEY PASSPHRASE ON ALL JUNIPER ATP APPLIANCE DEVICES
- VERIFYING CONFIGURATIONS
- ACCESSING THE JUNIPER ATP APPLIANCE CENTRAL MANAGER WEB UI
- SETTING SSH HONEYPOT DETECTION
- MANAGER OF CENTRAL MANAGERS (MCM)

Welcome to the Juniper Advanced Threat Prevention Appliance All-in-One Quick Start Guide.

Juniper ATP Appliance's continuous traffic-monitoring Collectors and multi-platform threat Detonation Engines provide context-aware inspection, detection, and intelligence. Managed by the Juniper ATP Appliance Central Manager, the All-in-One system inspects network traffic, extracts HTTP web and email objects, then detonates and analyzes potential malware threats. Juniper ATP defines threat severity specific to your environment. Results are reported through the Central Manager Web UI along with real-time mitigation actions that reach all the way to the enterprise endpoint. SIEM integration is also supported.

Use this guide to perform initial setup of the combined "All In One" Central Manager/Core/Collector Juniper ATP Server. Refer to the respective Quick Start Guides for separate Juniper ATP Appliance Traffic Collector(s) servers and Mac OS X Engine Secondary Core installations.

## Extensible Installations

Juniper ATP Appliance Server components can be installed as a single "All in One" appliance, or installed separately as distributed devices for wider network visibility.

Juniper ATP Appliance For Windows Detection	Combined Core Engine/Central Manager & Traffic Collector Server – An "All In One" Server Appliance
For Mac and Windows Detection	An All-in-One Core Server Appliance with a separate, connected Mac OS X Secondary Core

## 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:

- Configure outgoing access from the Juniper ATP Appliance Core eth0 management interface to the enterprise SMTP server, DNS servers, PAN or SRX Firewalls, BlueCoat or CarbonBlack servers, and

logging/SIEM servers.

- Be sure any additional distributed Collector(s) can communicate with the Core/Central Manager over port 443.
- Configure a management network proxy, or an “inside” or “outside” SPAN-traffic proxy using the CLI “set proxy” commands; refer to the Juniper Advanced Threat Prevention Appliance CLI Command Reference and Juniper Advanced Threat Prevention Operator’s Guide for more information.
- 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.

## Installing the Juniper ATP Appliance All-in-One Hardware Appliance

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

---

**NOTE** Two-Port Mac Mini requires a USB-to-NIC Adapter to create a configurable eth2 interface.

---

### To Install the Juniper ATP Appliance Server

1. Access and download the raw image for the All-in-One software 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.
2. 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.)
3. Connect the eth0 management and eth1 network interfaces on the server that will host the Juniper ATP software and confirm they are active links before beginning the software installation. Image installation requires at least an active eth0 connection.
4. Insert the USB drive containing the first bootable image to the USB port of the server that will host the Juniper ATP All-in-One software.
5. Use the down arrow keys to navigate the Boot Manager interface: select HARD DRIVE C: as the hard drive location, and down-arrow again to select the USB port containing the image.
6. At the menu display, select only this option: INSTALL Juniper ATP SOFTWARE.
7. Follow the prompt to remove the USB; the system will reboot itself. This reboot may take up to 20 minutes.
8. After reboot, the Juniper ATP CLI prompt appears. At the CLI, log in to the Juniper ATP CLI with the username `admin` and the password `1JATP234`.
9. 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

## Configuring the Juniper ATP Appliance All-in-One System

If you are powering up an All-in-One system in order to change initial configuration settings, you will need to log in as described immediately below.

The Juniper ATP Appliance Configuration Wizard steps you through initial configuration of the Juniper ATP Appliance All-in-One system. To exit the CLI, type `exit`.

### Logging into the Juniper ATP Appliance All-in-One 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`.

## Using the Configuration Wizard

Configuration Wizard Prompts	Customer Response Actions
<p>Use DHCP to obtain the IP address and DNS server address for the administrative interface (Yes/No)?</p> <p>Note: Only if your DHCP response is no, enter the following information when prompted:</p> <ul style="list-style-type: none"> <li>a. Enter a gateway IP address and netmask for this management (administrative) interface:</li> <li>b. Enter primary DNS server IP address.</li> <li>c. Do you have a secondary DNS Server (Yes/No).</li> <li>d. Do you want to enter the search domains?</li> <li>e. Enter the search domain (separate multiple search domains by space):</li> </ul> <p>Restart the administrative interface (Yes/No)?</p>	<p>We strongly discourage the use of DHCP addressing for the eth0 interface because it changes dynamically. A static IP address is preferred.</p> <p>Recommended: Respond with no:</p> <ul style="list-style-type: none"> <li>a. Enter a gateway IP X.X.X.X and quad-tuple netmask using the form 255.255.255.0 (no CIDR format).</li> <li>b. Enter the primary DNS IP address</li> <li>c. If yes, enter the IP address of the secondary DNS server.</li> <li>d. Enter yes if you want DNS lookups to use a specific domain.</li> <li>e. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com</li> </ul> <p>Enter yes to restart with the new configuration settings applied.</p>
Enter a valid hostname.	<p>Type a unique hostname when prompted; do not include the domain. A hostname should not include any spaces; for example: juniper-atpl</p>

Configuration Wizard Prompts	Customer Response Actions
<p>[OPTIONAL]</p> <p>If the system detects a Secondary Core with an eth2 port, then the alternate CnC exhaust option is displayed:</p> <p>Use alternate-exhaust for the analysis engine exhaust traffic (Yes/No)?</p> <p>Enter IP address for the alternate-exhaust (eth2) interface:</p> <p>Enter netmask for the alternate-exhaust (eth2) interface: (example: 255.255.0.0)</p> <p>Enter gateway IP Address for the alternate-exhaust (eth2) interface: (example:10.6.0.1)</p> <p>Enter primary DNS server IP Address for the alternate-exhaust (eth2) interface: (example: 8.8.8.8)</p> <p>Do you have a secondary DNS server for the alternate-exhaust (eth2) interface?</p> <p>Do you want to enter the search domains for the alternate-exhaust (eth2) interface?</p> <p>Note: A complete network interface restart can take more than 60 seconds</p>	<p>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 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>

NOTE: The remaining Wizard prompts are specific to Collector or Secondary device configurations.



Configuration Wizard Prompts	Customer Response Actions
Enter the following server attributes: Is this a Central Manager device:	Enter Yes; the system will auto-set IP 127.0.0.1 as the All-in-One CM IP address.
Device Name: (must be unique)	Enter the Juniper ATP Collector Host Name; this identifies the Collector in the Web UI.
Device Description	Enter a device Description
Device Key PassPhrase	Enter a user-defined PassPhrase to be used to authenticate the Core to the Central Manager.
NOTE: Remember this passphrase and use it for syncing all distributed devices!	

**NOTE** Enter CTRL-C to exit the Configuration Wizard at any time. If you exit without completing the configuration, you will be prompted again whether to run the Configuration Wizard. You may also rerun the Configuration Wizard at any time with the CLI command `wizard`. Please refer to the Juniper ATP Appliance CLI Command Reference for further information regarding the Juniper ATP Appliance Server command line.

## Setting the Same Device Key Passphrase on all Juniper ATP Appliance Devices

The same device key must be set on all Juniper ATP Appliance devices 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.

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

## Verifying Configurations

To verify interface configurations, use the following CLI commands (refer to the CLI Command Reference Guide for more information):

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 (diagnosis)# show device collectorstatus	Display All-in-One Collector statistics
JATP (server)# ping x.x.x.x	Ping connected devices.

CLI Mode & Command	Purpose
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).
JATP (server)# shutdown	Shutdown before moving a devices to a different location, or to perform server room maintenance etc

NOTE: Be sure to refer to the Juniper ATP 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

**NOTE** 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.

---

**NOTE** Be sure any distributed devices (additional Collectors or Mac OS X Engines) connected to the All-in-One system are configured with the same device key as defined by the CLI command `set passphrase`. If you do not set the same passphrase on all devices, you will not be able to see the Collector or the Mac OS X Engine in the Web UI.

---

## To Log in to the Central Manager Web UI

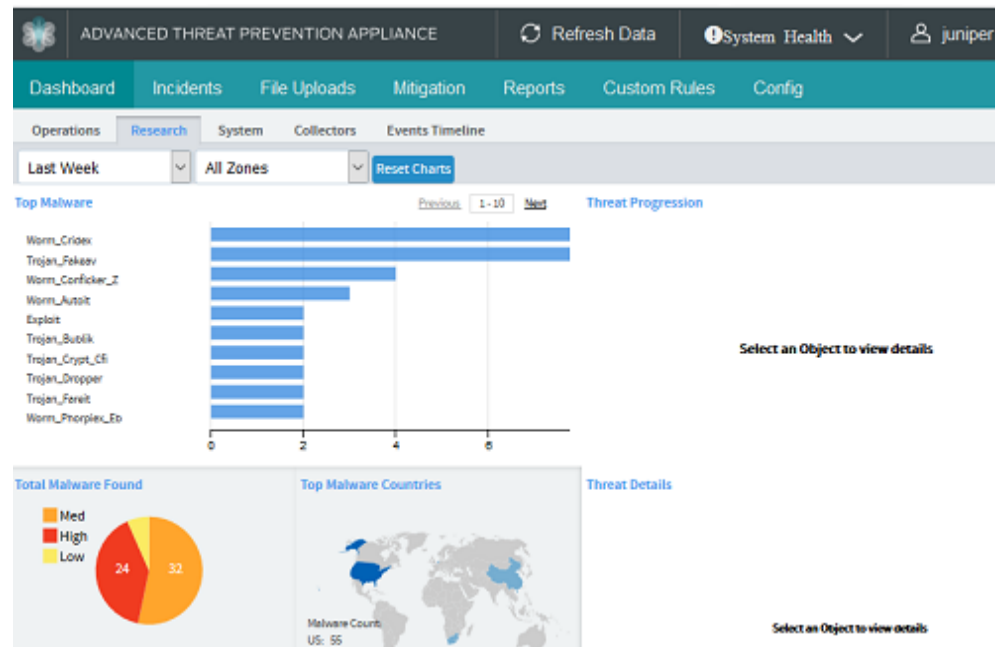
1. In the Juniper ATP Login window, enter the default username `admin` and the password `juniper`.
2. When prompted to reset the password, re-enter the password `juniper` as the "old" password, and enter a new password (twice).

**NOTE** 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.

Figure 1 Central Manager Dashboard

Web UI  
Navigation Tabs

- **Dashboard**  
Review in-context malware summaries lateral progressions and trends: Operations, Research, System, Collectors, Events Timeline
- **Incidents**  
View detected incidents and their behaviors
- **File Uploads**  
Upload files for analysis
- **Mitigation**  
Perform immediate threat verification & mitigation



The Juniper ATP Appliance CM Dashboard provides in-context and aggregated malware detection information as well as system status and health information. Additional configurations are made from the Configuration tab. Refer to the Operator's Guide for more information.

## 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.

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.

## Manager of Central Managers (MCM)

The Juniper ATP Appliance Manager of Central Managers (MCM) is a device that provides a Web UI management console 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.