

Juniper Advanced Threat Prevention Appliance

Mac OS X Quick Start Guide

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

408-745-2000

www.juniper.net

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

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

Juniper Advanced Threat Prevention Mac OS X 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
- SPECIFICATIONS & INSTALLATION PREREQUISITES
- CONFIGURING THE JUNIPER ATP APPLIANCE FOR MAC OS X
- SETTING THE SAME DEVICE KEY PASSPHRASE ON ALL JUNIPER ATP APPLIANCES
- VERIFYING CONFIGURATIONS AND TRAFFIC FROM THE MAC MINI CLI
- UPGRADING A MAC MINI DETECTION SYSTEM ISO
- VIEWING MAC OS X DETECTION AT THE JUNIPER ATP APPLIANCE WEB UI
- BE SURE ALL JUNIPER ATP APPLIANCES 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 IN THE CENTRAL MANAGER WEB UI. REFER TO SETTING THE SAME DEVICE KEY PASSPHRASE ON ALL JUNIPER ATP APPLIANCES. SPECIAL CHARACTERS USED IN CLI PARAMETERS MUST BE ENCLOSED IN DOUBLE QUOTATION MARKS.
- WHAT TO DO NEXT?

Welcome to the Juniper ATP Appliance Quick Start for Mac Mini. The Juniper ATP Appliance does not ship on Mac Mini hardware. The customer is responsible for obtaining a Mac Mini device.

The Juniper ATP Appliance extends its Windows platform malware analysis products to include seamless integration of Mac OS X traffic monitoring and malware detection. The MAC OS X detonation chamber runs on a Mac Mini and is supplied by Juniper ATP Appliance as a direct Secondary Core extension of its Core/Central Manager Server for detecting both known and unknown threats.

When linked logically to the Core, the Juniper ATP Appliance Collectors inspect all network traffic for malware objects; they extract and send objects to the CM Core for distribution to the Windows or Mac Detection Engines. The Mac OS detonates and analyzes all Mach-O executables, and any archive containing a Mach-O object, as well as any downloaded apps. Mac OS threats and malware are reported in the Juniper ATP Appliance CM Web UI similar to detected Windows events, and include corresponding context-specific Mitigation options.

This document assumes you have already installed and configured the Juniper ATP Appliance Core/CM or All-in-One Server.

Extensible Installations

Deployment and configuration of the Juniper ATP Appliance Mac Mini Detection Engine is a simple and straightforward procedure: plug-in a keyboard and mouse, and enter the IP address of the Juniper ATP Appliance Central Manager Core (CM) when prompted by the Configuration Wizard. Multiple clustered Mac Mini devices can be deployed, as needed, depending on enterprise traffic load.

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).

Specifications & Installation Prerequisites

- SPECIFICATIONS
CPU: Intel Core i5 Dual-Core 2.6GHz | Memory: 16GB RAM 1600MHz LPDDR3 SDRAM | HDD: 1 TB SATA @5400rpm [Juniper does not support Fusion drives with current software.] | Additional NIC required for collection or cooking exhaust: use an Apple USB Ethernet Adapter Part number: MC704LL/A | Mini Display Port to VGA Adapter Part number MB572Z/B

- For initial configuration, have available a mini-DV or mini-display cable for connecting a monitor to the Mac Mini Device running Juniper ATP software, and use any USB keyboard for entering configuration information. Use an HDMI connection or a DVI adapter on the Mac for a video connection.
- Use the provided AC power cable for connecting the Mac Mini power supply.

Installing Juniper ATP Mac OS Software on Mac Mini Hardware

1. Unpack the Mac Mini device.
2. Connect the power cable and power up the appliance. Allow a few minutes for the Juniper ATP Appliance software to boot up and be ready to configure.
3. Connect a monitor and USB keyboard to the Mac Mini to perform the initial configuration.
4. Connect the Ethernet port eth0 to the enterprise management network. You are ready to configure the Mac OS X Engine.
5. Connect the (optional) alternate analysis engine exhaust eth2 interface via a NIC-to-USB adapter to your monitoring network. This keeps analysis engine traffic to CnC servers, for example, off the management network.

Configuring the Juniper ATP Appliance for Mac OS X

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

To Configure the Appliance

1. At the login prompt, enter the default username `admin` and the password `1JATP234`. Review the displayed EULA and press `q` to continue.
2. When prompted to accept the Juniper ATP Appliance End User License Agreement (EULA), enter `yes`. Configuration cannot continue until the EULA is accepted.
3. When prompted with the query “Do you want to configure the system using the Configuration Wizard (Yes/No)?”, enter `yes`.
4. 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.
5. Respond to the Configuration Wizard questions using the following response options

Configuration Wizard

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 for the eth0 interface because it changes dynamically. A static IP address is preferred. Recommended: Respond with no:
Note: Only if your DHCP response is no, enter the following information when prompted: a. IP address b. Netmask c. Enter a gateway IP address for this management (administrative) interface: d. Enter primary DNS server IP address. e. Do you have a secondary DNS Server (Yes/No). f. Do you want to enter the search domains? g. Enter the search domain (separate multiple search domains by space): Restart the administrative interface (Yes/No)?	Enter a gateway IP X.X.X.X and quad-tuple netmask using the form 255.255.255.0 (no CIDR format). a. Enter an IP address b. Enter a netmask c. Enter a gateway IP address. d. Enter the DNS server IP address e. If yes, enter the IP address of the secondary DNS server. f. Enter yes if you want DNS lookups to use a specific domain. g. Enter search domain(s) separated by spaces; for example: example.com lan.com dom2.com Enter yes to restart with the new configuration settings applied.
Enter a valid hostname.	Type a hostname when prompted; do not include the domain; for example: macosx
Enter the following server attributes: Central Manager (CM) IP Address: Device Name: (must be unique) Device Description Device Key PassPhrase NOTE: Remember this passphrase and use for all distributed devices!	Enter the IP address of the Juniper ATP Appliance CM external IP address, not the loopback. Enter a Mac Mini Device running Juniper ATP software Name; this identifies the Mac Mini in the Web UI. Enter a device Description Enter the same PassPhrase used to authenticate the Mac Mini to the Central Manager.

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 Operator's Guide for further information regarding the Juniper ATP Appliance command line.

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

Setting the same Device Key Passphrase on all Juniper ATP Appliances

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 Mac Mini CLI

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

Table 1 Verify interface configurations

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 eth0]
JATP (server) # ping x.x.x.x	Ping connected devices.
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 CLI Command Reference Guide for more information. Special characters used in CLI parameters must be enclosed in double quotation marks.

TIP A 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).

Upgrading a Mac Mini Detection System ISO

Use the following procedure to upgrade the Mac OSX Detection System ISO.

1. Copy the bootable image to a USB drive; Kingston USB flash drives are recommended.
2. Insert the USB drive into the MAC.
3. Connect the HDMI console to a Windows system.
4. Reboot the Mac Mini system from the console using the CLI 'reboot' command.

5. Hold down the keyboard "Alt" key after hearing the Mac's startup chime.
6. Choose option 2 when prompted to make a choice.
7. Hold down the keyboard 'C' key to directly boot the image from the USB drive.

NOTE The upgrade process will take approximately 15-20 minutes.

Viewing Mac OS X Detection at the Juniper ATP Appliance 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 a web browser address field, and accept the SSL certificate when prompted. You are always required to log into the CM Web UI.

To Log in to the Central Manager

1. In the Juniper ATP Appliance 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 for both Windows and Mac OS X, and provides system status and health information. Additional configurations are made from the Config tab. Refer to the Juniper ATP Appliance Operator's Guide for more information.
4. The status of the Mac Secondary Core can be viewed by going to the Config Tab of the Juniper ATP Appliance Central Manager and selecting System Settings>Secondary Cores from the left panel Web UI menu.

The Central Manager updates detection results every 5 minutes; refresh the Web UI to check the Dashboard and Threats tabs for Mac malware events.

The Juniper ATP Appliance CM Dashboard provides in-context and aggregated malware detection information as well as system status and health

NOTE Be sure all Juniper ATP Appliances 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 in the Central Manager Web UI. Refer to [Setting the same Device Key Passphrase on all Juniper ATP Appliances](#). Special characters used in CLI parameters must be enclosed in double quotation marks.

What to Do Next?

- Navigate to the Configuration tab and select Licensing from the left panel; upload your license key (obtained from your sales representative).
- Use the Central Manager (CM) Web UI Dashboard and Configuration>Secondary Cores 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.
- 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 Traffic Collector Quick Start Guide for information about installing a small form factor Mac Mini Collector.

- Refer to the Juniper ATP Appliance All-in-One System Quick Start Guide for information about installing a Mac Mini Detection Engine to the All-In-One system.
- Review the Juniper ATP Appliance Core/CM Quick Start Guide for information about the Core/CM platform installation and configuration.
- Refer to the Juniper ATP Appliance Operator's Guide for more information about Juniper ATP Appliance products and usage.
- Refer to the Juniper ATP Appliance Manager of Central Managers (MCM) User's Guide for information about managing distributed Central Managers.
- Review the Juniper ATP Appliance CLI Command Reference for usage of the command line interface for all Juniper ATP Appliance devices or software products.
- Refer to the Juniper ATP Appliance HTTP API Reference for information about accessing and managing Juniper ATP Appliance advanced threat detection data using APIs, including processing data, device and software configuration.
- Refer to the Juniper ATP Appliance CEF Logging Support for SIEM Integration Guide for information about CEF logging.