




Juniper Advanced Threat Prevention Appliance—Private Mode



Modified: 2019-06-11

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.

Juniper Advanced Threat Prevention Appliance—Private Mode
Copyright © 2019 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
	Creating a Service Request with JTAC	xiii
Chapter 1	Overview and Enable CLI	15
	JATP Private Mode CLI Commands	15
Chapter 2	Download and Install Updates	17
	Download and Install Updates in JATP Private Mode	17
	JATP Private Mode Software Package Bundle	17
	Manually Upload Software Updates Using the UI	17
	Manually Upload Software Updates Using the CLI	19
Chapter 3	Private Mode Functionality	21
	JATP Features Affected by Private Mode	21

List of Figures

Chapter 2	Download and Install Updates	17
	Figure 1: JATP Private Mode Navigate to Software Update	18
	Figure 2: JATP Private Mode Upload Software Update	19

List of Tables

	About the Documentation	ix
	Table 1: Notice Icons	x
	Table 2: Text and Syntax Conventions	x
Chapter 1	Overview and Enable CLI	15
	Table 3: JATP Private Mode CLI Commands	15

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>

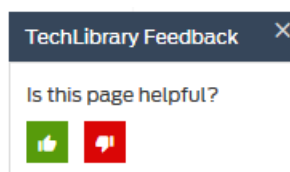
Table 2: Text and Syntax Conventions (continued)

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 Juniper Care or Partner Support Services 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/>
- Create a service request online: <https://myjuniper.juniper.net>

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- 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://support.juniper.net/support/requesting-support/>.

CHAPTER 1

Overview and Enable CLI

- [JATP Private Mode CLI Commands on page 15](#)

JATP Private Mode CLI Commands

Use JATP in an air gapped environment with no Internet access or insecure network access by enabling Private Mode. When in Private Mode, features that require the Internet are disabled and offline-specific commands and UI pages are enabled.

Private Mode is enabled through the CLI. When operating in Private Mode, the JATP UI will display text informing administrators that JATP is in Private Mode.

Note the following about JATP Private Mode:

- Software and content updates are manually downloaded and applied.
- New Private Mode-specific CLI commands are available, as well as UI pages.
- Several Internet dependent features are unavailable. See [“JATP Features Affected by Private Mode” on page 21](#).
- No malware exhaust traffic is allowed out through the management interface. Other traffic can still leave the JATP device through the exhaust interface if it is configured.
- If you enable Private Mode on the Core/Central Manager, All-In-One, or Manager of Central Managers, all secondary devices get updated automatically.

Use the following CLI commands for JATP Private Mode:

Table 3: JATP Private Mode CLI Commands

CLI Command	Purpose
<code>set private-mode enable on/off</code>	Enable/Disable Private Mode
<code>set private-mode update copy File-URL</code>	Copy update files from an internal staging server to the JATP device.

Table 3: JATP Private Mode CLI Commands (continued)

CLI Command	Purpose
set private-mode update start software/content/win10/win7/osx VERSION	<p>Set the update version and start the update process. Note that the update release can only be set forward and not backward (downgrades are not supported). In Private Mode, all software and content updates must be started manually. This is done to prevent incorrect provisioning of the uploaded update repository files.</p> <p>NOTE: You can run the “show private-mode update versions” command explained in this table, to check if the uploaded files have any dependencies that have not been met.</p> <p>(The repository referred to here and elsewhere is the directory in Core/CM devices where software and content images are copied.)</p>
show private-mode update copy	Check the status of the update.
show private-mode enabled	Display whether or not Private Mode is enabled.
show private-mode update versions	Show the available software and content update repositories that can be chosen for upgrading. This will also show the currently set release and the repository that is used for the update.
set autoupdate software on/off set autoupdate content on/off	Set “autoupdate” to “on” for software and content to allow connected secondary devices to automatically receive updates from Core devices.
set private-mode update delete	You can delete the update files to free up more disk space.

Related Documentation • [Download and Install Updates in JATP Private Mode on page 17](#)

CHAPTER 2

Download and Install Updates

- [Download and Install Updates in JATP Private Mode on page 17](#)

Download and Install Updates in JATP Private Mode

Use the following information to download and apply software updates when using JATP in Private Mode.

- [JATP Private Mode Software Package Bundle on page 17](#)
- [Manually Upload Software Updates Using the UI on page 17](#)
- [Manually Upload Software Updates Using the CLI on page 19](#)

JATP Private Mode Software Package Bundle

All of the software listed below is bundled together into a single package file to upload to the JATP Core.

- JATP OS software—Includes the JATP software packages.
- Security patches—Includes the security patches of the base open source software provided by Ubuntu community.
- Third-party software—Includes the third-party open source software packages.
- SSH Honeypot image
- Sky ATP API engine image

Manually Upload Software Updates Using the UI

The manual installation of software updates is only available in Private Mode. When not in Private Mode, JATP updates occur automatically.

In Private Mode, you can use the JATP UI or the CLI to install an update.

Update using the JATP UI:

1. Download the update files from the Juniper download portal, <https://support.juniper.net/support/downloads/>.

- In the UI, navigate to **Config > System Profiles > ATP Private Mode Update** and select **Upload File** to upload a file bundle or image file. A progress bar is shown when the upload begins. Note that if you close the file upload dialog box or close the browser tab, the file upload activity will be aborted.

When the file upload is complete, the uploaded file is listed in the UI with information such as type, version and date of the upload (That is, if the version of the uploaded file is newer than the currently installed version).

Figure 1: JATP Private Mode Navigate to Software Update

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health J-ATP Admin

Dashboard Incidents File Uploads Mitigation Reports Custom Rules **Config**

Notifications

System Profiles

Password Reset

Roles

Zones

Users

SAML Settings

RADIUS Settings

System Settings

Certificate Management

GSS Settings

Web Collectors

SRX Settings

Email Collectors

Secondary Cores

Golden Image VMs

Licensing

ATP Private Mode Update

Upload Update Files

ATP Private Mode: ON

Content Version: 5.0.6.437

Software Version: 5.0.6.1298

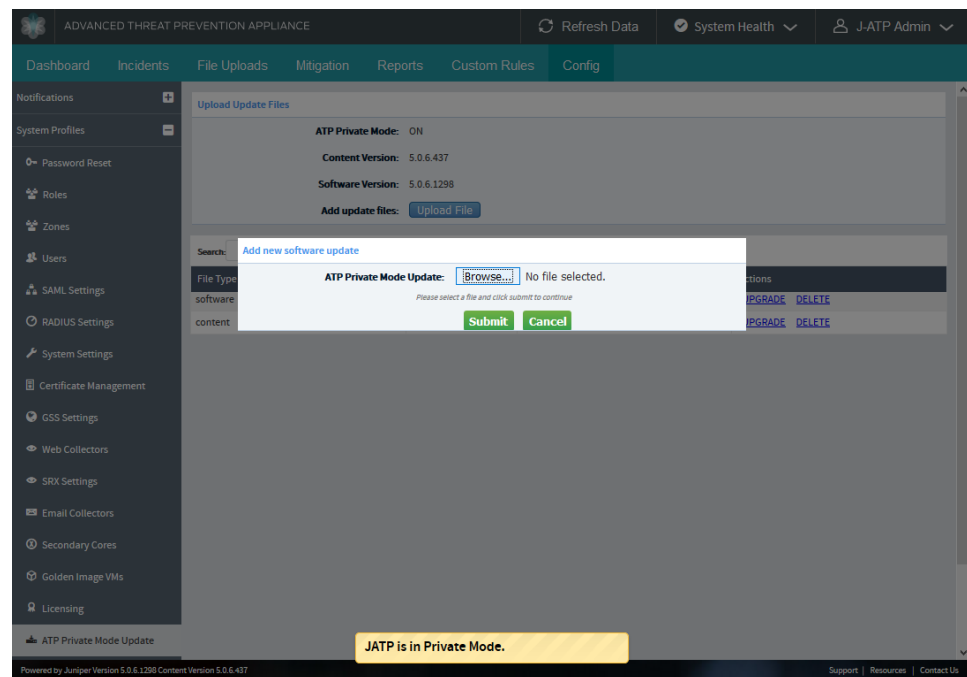
Add update files: [Upload File](#)

Search:

File Type	Version	Status	Actions
software	5.0.6.1298	available	UPGRADE DELETE
content	5.0.6.437	available	UPGRADE DELETE

JATP is in Private Mode.

Figure 2: JATP Private Mode Upload Software Update



- Once the upload is complete, you can manually begin the update by clicking the **Upgrade** link next to the uploaded file in the **Config > System Profiles > ATP Private Mode Update** window.

You can also delete the uploaded file from the same window.



NOTE: It is recommended that you always create a fresh configuration backup after updating to a new software release.

Manually Upload Software Updates Using the CLI

Another method for updating JATP in Private Mode is to copy the update file to the JATP device from a staging server using the JATP CLI.

- Run the following command to allow the JATP device access to the staging server:

```
# set firewall whitelist add IP_ADDRESS_OF_STAGING_SERVER
```

- Download the update files from Juniper download portal to a staging server, <https://support.juniper.net/support/downloads/>.

- Run the following command to copy the update files to the JATP device:

```
set private-mode update copy FILE-URL
```

For example, **set private-mode update copy**
userabc@STAGING-SERVER-IP:FILE_PATH/jatp-update-5.2.tgz



NOTE: Note that only one update file can be uploaded at a time. The secure copy protocol (SCP) is used.

File uploads are processed in the background. Using the **show private-mode update copy** command, you can view the completion percentage of the upload.

4. Once the file upload completes, the update file preparation process starts and performs the following tasks:
 - Check and verify the completeness and the integrity of the file.
 - Check if the same update file already exists in the system. If so, remove the file.
 - Check if the uploaded file is an older version of the existing installed software or content. If so, remove the uploaded file.
 - Decompress the file and move it to the correct location.
 - Verify the version information for the software or content file.
 - Save the state related information in the database.
5. Once the upload is complete (check status with the **show private-mode update copy** command), you can manually begin the update with the following example command:

set private-mode update start software/content/win10/win7/osx VERSION



NOTE: The repository is not available for connected secondary devices (such as Web Collectors and Secondary Cores) to download until the JATP Core has finished the software upgrade process.



NOTE: It is recommended that you always create a fresh configuration backup after updating to a new software release.

Related Documentation • [JATP Features Affected by Private Mode on page 21](#)

CHAPTER 3

Private Mode Functionality

- [JATP Features Affected by Private Mode on page 21](#)

JATP Features Affected by Private Mode

When operating in Private Mode, the following JATP functionality may be viewable in the UI but greyed-out and unavailable due to no Internet connection.

- Internet Health Checks
- GSS Configuration and Remote Support
- VirusTotal Lookup from the UI (Malware Events)
- EICAR file download tests

Also note the following:

- Email Collection for Gmail and Office365 requires Internet access and therefore will not function in an air gapped environment.
- No Malware Exhaust Traffic is allowed out through the management interface.
- Support Ticket Generation from the UI (Malware Events) requires Internet access and therefore will not function in an air gapped environment.

For support ticket generation, rather than submit tickets to the GSS cloud service directly, download the support ticket as a zip file. Email that ticket to the Juniper Threat Lab team using the email address **EXT-JATP-JTL-Support@juniper.net**.



NOTE: Please report all other issues in the usual way. See the “Requesting Technical Support” section in the Release Notes for details.

Related Documentation

- [JATP Private Mode CLI Commands on page 15](#)

