

# Juniper Advanced Threat Prevention Appliance Release Notes

Release 5.0.7  
January  
Revision 1

<b>Contents</b>	<a href="#">Juniper Advanced Threat Prevention Appliance Release Notes   2</a>
	<a href="#">Introduction   2</a>
	<a href="#">New and Changed Features   2</a>
	<a href="#">Remote Support Secret Key Integration   3</a>
	<a href="#">Reset the Administrator Password   3</a>
	<a href="#">Audit Logs for CLI Activity and Software, Content, and Fast-Content Update   3</a>
	<a href="#">Domain Transition from cloud.cyphort.com to gss.junipersecurity.net   3</a>
	<a href="#">Add Proxy IP Addresses for SRX Series Devices   4</a>
	<a href="#">Integration of JATP with Policy Enforcer   4</a>
	<a href="#">Software Installation and Upgrade Notes   5</a>
	<a href="#">Software Upgrades—JATP Private Mode   5</a>
	<a href="#">Software Upgrades   5</a>
	<a href="#">Wipe the Device   6</a>
	<a href="#">Product Information: Behaviors and Notes   6</a>
	<a href="#">Documentation Feedback   6</a>
	<a href="#">Requesting Technical Support   7</a>
	<a href="#">Self-Help Online Tools and Resources   7</a>
	<a href="#">Creating a Service Request with JTAC   8</a>
	<a href="#">Revision History   8</a>

# Juniper Advanced Threat Prevention Appliance Release Notes

## IN THIS SECTION

- [Introduction | 2](#)

## Introduction

The Juniper Networks<sup>®</sup> Advanced Threat Prevention Appliances (JATP Appliances) provide continuous, multistage detection and analysis of Web, e-mail, and lateral spread traffic moving through the network. A JATP Appliance collects information from multiple attack vectors, using advanced machine learning and behavioral analysis technologies to identify advanced threats in as little as 15 seconds. Those threats are then combined with data collected from other security tools in the network, analyzed, and correlated, creating a consolidated timeline view of all malware events related to an infected host. After threats are identified, “one-touch” policy updates are pushed to inline tools to protect against a recurrence of advanced attacks.

## New and Changed Features

## IN THIS SECTION

- [Remote Support Secret Key Integration | 3](#)
- [Reset the Administrator Password | 3](#)
- [Audit Logs for CLI Activity and Software, Content, and Fast-Content Update | 3](#)
- [Domain Transition from cloud.cyphort.com to gss.junipersecurity.net | 3](#)
- [Add Proxy IP Addresses for SRX Series Devices | 4](#)
- [Integration of JATP with Policy Enforcer | 4](#)

## Remote Support Secret Key Integration

The customer support password is generated using two secret keys—one automatically obtained by Juniper Networks Support from the JATP device when remote support is enabled and another from Juniper Networks. When the JATP device is online, these keys are synchronized with the Global Security Services (GSS) automatically. In Private Mode, you must manually share the JATP device secret key with Juniper Networks Support. As part of this feature, we've moved the option to enable remote support from the System Settings and GSS sections of the JATP Web UI to the new Remote Support section. We've also provided an option to specify the time duration for the remote support session.

See the [Operator's Guide](#) for details.

## Reset the Administrator Password

To help you reset the administrator password, we've created a username that does not require a password. You must have physical access to the appliance to log in as this user and execute a reset password command.

See the [All-in-One Quick Start Guide](#) for details.

## Audit Logs for CLI Activity and Software, Content, and Fast-Content Update

In addition to viewing UI users in the audit logs, you can now also view the following information in the audit logs, under the **Reports** section in the Web UI:

- CLI users (admin and recovery-admin)
- Software, content, and fast-content update

See the [Operator's Guide](#) for details.

## Domain Transition from cloud.cyphort.com to gss.junipersecurity.net

Starting in JATP Release 5.0.7, we've changed the GSS services domain from \*.cloud.cyphort.com to \*.gss.junipersecurity.net. You must change your existing firewall rules to allow outbound traffic to the new \*.gss.junipersecurity.net domain. Both the domains will be valid during the transition to the new domain, but we will phase out \*.cloud.cyphort.com in the future. We recommend that you transition to the new domain as soon as possible.

See the [Operator's Guide](#) for details.

## Add Proxy IP Addresses for SRX Series Devices

If you are using a proxy with the SRX Series device, JATP may incorrectly identify the proxy IP address as the endpoint address. You can now add the proxy IP addresses to the JATP UI and make JATP aware of these addresses. JATP is then able to identify the correct endpoint IP addresses for you..

See the [Juniper Advanced Threat Prevention Appliance Integration with the SRX Series Device Guide](#) for details.

## Integration of JATP with Policy Enforcer

Policy Enforcer, a component of Junos Space Security Director, provides centralized, integrated management of all your security devices (both physical and virtual), giving you the ability to combine threat intelligence from different solutions and act on that intelligence from one management point.

Policy Enforcer provides the following features:

- Pervasive security—Combines security features and intelligence from devices across your network, including switches, routers, and firewalls, to create a secure fabric that leverages information you can use to create policies that address threats in real time and into the future. With monitoring capabilities, JATP-integrated Policy Enforcer can also act as a sensor, providing visibility for intra- and internetwork communications.
- User intent-based policies—Creates policies according to logical business structures, such as users, user groups, geographical locations, sites, tenants, applications, or threat risks. This allows network devices (switches, routers, firewalls, and other security devices) to share information, resources, and when threats are detected, remediation actions within the network.
- Threat intelligence aggregation—Gathers threat information from multiple locations and devices, both physical and virtual, as well as third-party solutions.

We've added a MAC address column to the Infected Hosts page as part of the JATP-Policy Enforcer integration. Policy Enforcer provides the MAC address of the host, but other devices, such as the SRX Series services gateways, do not provide the MAC address. Therefore, this column will contain no information if the MAC address cannot be obtained for the infected host.

See the [Policy Enforcer](#) guide for details.

# Software Installation and Upgrade Notes

## IN THIS SECTION

- [Software Upgrades—JATP Private Mode | 5](#)
- [Software Upgrades | 5](#)
- [Wipe the Device | 6](#)

## Software Upgrades—JATP Private Mode

In Private Mode, JATP upgrades must be done manually. See the [Juniper Advanced Threat Prevention Appliance—Private Mode Guide](#) for details.

## Software Upgrades

Software upgrades to the Juniper ATP Appliance occur automatically. The appliance checks for new software and content updates each day at regular intervals and automatically applies those updates. See the [Operator's Guide](#) for details.



### WARNING:

- Unless you are using JATP in Private Mode, you should not perform a manual software upgrade of the Juniper ATP Appliance. If you want a particular software version installed on the appliance, contact Juniper Networks Technical Assistance Center (JTAC) for assistance.
- For existing installations, ISO files posted to Juniper.net should only be used to recover from critical failures under exceptional circumstances with the guidance of JTAC or a sales engineer.
- If your appliance was reimaged with an ISO downloaded from Juniper.net, we recommend that you open a case with JTAC to ensure the device is registered correctly for updates.

## Wipe the Device

To wipe the device, it is recommended you use DBAN software. Those instructions can be found here: <https://www.lifewire.com/how-to-erase-a-hard-drive-using-dban-2619148>

## Product Information: Behaviors and Notes

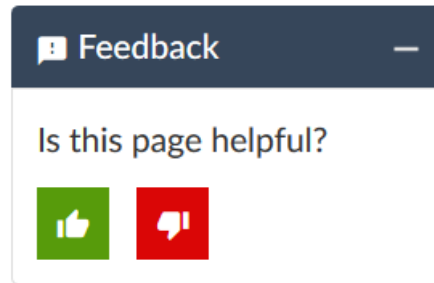
This section lists information about product behavior for the hardware and software of the Juniper ATP appliance.

- When integrating JATP with an SRX Series device, you cannot use fxp0 interfaces to communicate with JATP. You must use a separate revenue interface. See the [JATP and SRX Series Integration Guide](#) for details.
- Backup and Restore is only for the Web UI configuration and does not include all incidents and events.
- Alerts are private to the user who created them. It is possible to add users (or groups) other than the author to alerts. This can result in users seeing unexpected alerts that they cannot see in their own views.
- The Juniper ATP virtual appliance does not have VMWare tools installed. You must power off the appliance for migration and/or cloning using the CLI.
- Alerts for command and control server (CnC or C2) traffic are only sent on the initial occurrence to avoid alert fatigue.
- The system does not enforce resource requirements for disk, RAM, and CPU. Although installations with limited resources might initially work, they will eventually exhibit issues.
- Both the Juniper ATP Appliance Core and All-in-One devices require Internet access. Other products might report a health alert for “Internet,” but you can disregard those alerts.
- You can deploy the JATP appliance as an e-mail collector. There is no separate orderable SKU for this deployment, but any JATP appliance may be repurposed for this function.

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using 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](mailto: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/>
- 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/>.

## Revision History

January 2020—Revision 1—JATP

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

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.