

Juniper Advanced Threat Prevention Appliance Release Notes

Release 5.0.5
March
Revision 1

Contents

Juniper Advanced Threat Prevention Appliance Release Notes	2
Introduction	2
New and Changed Features	2
Zone Support for SRX Series Devices	2
Support for Windows 10 Sandboxing	2
Software Installation and Upgrade Notes	3
Software Upgrades	3
Wipe the Device	3
Product Information: Behaviors and Notes	3
Documentation Feedback	4
Requesting Technical Support	4
Self-Help Online Tools and Resources	5
Creating a Service Request with JTAC	5
Revision History	5

Juniper Advanced Threat Prevention Appliance Release Notes

- [Introduction](#)

Introduction

The Juniper Advanced Threat Prevention Appliance provides continuous, multistage detection and analysis of Web, e-mail, and lateral spread traffic moving through the network. It 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. Once threats are identified, “one-touch” policy updates are pushed to inline tools to protect against a recurrence of advanced attacks.

New and Changed Features

- [Zone Support for SRX Series Devices on page 2](#)
- [Support for Windows 10 Sandboxing on page 2](#)

Zone Support for SRX Series Devices

MSSPs can now add SRX Series devices to zones along with traffic collectors. Once added to a JATP zone, multi-tenant MSSPs can manage SRX Series incidents per zone and tenant. See the [JATP Integration with the SRX Series Device](#) for details.

Support for Windows 10 Sandboxing

This release supports Windows 10 sandboxing (in addition to Windows 7) for behavior analysis. For JATP virtual appliances (vJATP), Windows 10 sandboxing requires “nested hypervisor support” or “guest VM hypervisor support” enabled from vSphere.

Before You Begin

- The VM should be upgraded to ESXi 6 or later (VMWare version 11).
- Shut down the vJATP VM.

To enable nested virtualization, the “hardware-assisted virtualization” capabilities need to be exposed to the VM, in this case vJATP.

1. Once the VM is powered off, use the vSphere web client to navigate to the **Compatibility** option and select **Upgrade VM Compatibility**.
2. Once the VM compatibility upgrade finishes, use the vSphere web client to navigate to the **Processor Settings** screen. Select the check box next to **Expose hardware-assisted virtualization to the guest operating system**.
3. Click **OK**.

Software Installation and Upgrade Notes

- [Software Upgrades on page 3](#)
- [Wipe the Device on page 3](#)

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:

- 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.

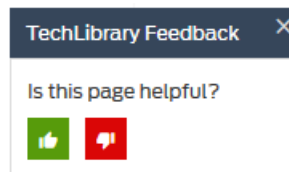
- When integrating JATP with an SRX Series device, you cannot use fxp0 interfaces to communicate with JATP. You must use a separate revenue interface. See the [JATP and SRX Series Integration Guide](#) for details.
- Backup and Restore is only for the Web UI configuration and does not include all incidents 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. 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

March 2019—Revision 1—JATP

Copyright © 2019 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.