

Use these release notes to learn about new features and known issues in this release.

# Juniper Advanced Threat Prevention Appliance 5.0.2 Release Notes

**Release 5.0.2**  
**June 2018**  
**Revision 2**

## **Contents**

New and Changed Features . . . . .	2
Support for Forcepoint SMC . . . . .	2
Integration with the SRX Series . . . . .	2
Product Information: Behaviors and Notes . . . . .	2
Documentation Feedback . . . . .	3
Requesting Technical Support . . . . .	3
Self-Help Online Tools and Resources . . . . .	4
Opening a Case with JTAC . . . . .	4
Revision History . . . . .	4

## New and Changed Features

---

This section lists the changes in the Juniper ATP Appliance for release 5.0.2.

- [Support for Forcepoint SMC on page 2](#)
- [Integration with the SRX Series on page 2](#)

### Support for Forcepoint SMC

Forcepoint NGFW Security Management Center (SMC) offers centralized management of Forcepoint Next Generation Firewalls across distributed network enterprises. With monitoring, logging, alerts, and reports, Forcepoint SMC provides a complete view of network security events to administrators. The Juniper ATP Appliance monitors and detects malicious IP addresses and the URLs that link to malware. Integration with Forcepoint SMC prevents users behind the Forcepoint firewall from accessing these IPs or URLs. Integration requires setup on JATP and Forcepoint SMC.

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

### Integration with the SRX Series

The Juniper Advanced Threat Prevention Appliance integrates with the SRX Series device to protect all hosts in your network against evolving security threats by employing JATP's threat detection software with a next-generation firewall system.

For this release, the SRX Series device integrates with the JATP Core to provide the following features:

- File scanning with global whitelists and blacklists.
- File scanning for administrator-created file profiles for specified file types.
- Feeds for infected hosts, command and control servers, and GeolIP.
- Email attachment scanning for SMTP and IMAP.

For this integration, configuration is required on both JATP and the SRX series device.

See [JATP and SRX Series Integration Guide](#)

## 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 the 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 may initially work, they will eventually exhibit issues.
- Both the Juniper ATP Appliance Core and All-in-One device require Internet access. Other products may report a health alert for "Internet," but you can disregard those alerts.
- The **setupcheck** command may show a failure on the WinXP sandbox image. This can be disregarded as it is no longer used.
- You can deploy the JATP700 appliance as an e-mail collector. There is no separate orderable SKU for this deployment, but any JATP700 appliance may be re-purposed for this function.

The following support Information is called out here for your reference. Note that the product documentation also contains support information. If there is a disparity, these release notes contain the most updated information.

- Only VMware versions 5.0, 5.5, and 6.0 are supported at this time.
- Only Windows 7 is supported for a Golden Image.

---

## 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 rating system—On any page of the Juniper Networks TechLibrary site at <https://www.juniper.net/documentation/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/documentation/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 <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: <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/>
- Open a case online in the CSC Case Management tool: <https://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 <https://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 <https://www.juniper.net/support/requesting-support.html>.

## Revision History

---

June 2018—Revision 2—Juniper Advanced Threat Prevention Appliance

Copyright © 2018 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.