

# Sky Advanced Threat Prevention Release Notes for Junos 15.1X49-D80 Release Notes

Release 15.1X49-D80  
March 2017  
Revision 1

## Contents

Sky Advanced Threat Prevention Release Notes . . . . .	2
Introduction . . . . .	2
Recommended Software Version . . . . .	2
New and Changed Features . . . . .	2
E-Mail Attachments . . . . .	2
SSL Proxy for Server Protection . . . . .	3
Changes in Behavior and Syntax . . . . .	3
HA Failover and Security Intelligence Daemon . . . . .	3
Match Condition . . . . .	4
Known Issues . . . . .	4
Documentation Feedback . . . . .	5
Requesting Technical Support . . . . .	6
Self-Help Online Tools and Resources . . . . .	6
Opening a Case with JTAC . . . . .	6
Revision History . . . . .	7

## Sky Advanced Threat Prevention Release Notes

---

- [Introduction](#)
- [Recommended Software Version](#)

### Introduction

Juniper Networks Sky ATP keeps your network free of sophisticated zero-day attacks and other unknown threats by delivering superior cloud-based protection, scanning ingress and egress traffic for malware and indicators of compromise.

Sky ATP employs a pipeline of technologies in the cloud to identify varying levels of risks, providing a higher degree of accuracy in threat prevention. It integrates with Juniper Networks SRX Series Services Gateways to deliver deep inspection, inline malware blocking, and actionable reporting.

Sky ATP's identification technology uses a variety of techniques to quickly identify a threat and prevent an impending attack. These methods include:

- Rapid cache lookups to identify known files.
- Dynamic analysis that involves unique deception techniques applied in a sandbox to trick malware into activating and self-identifying.

Additionally, machine-learning algorithms enable Sky ATP to adapt to and identify new malware in an ever-changing threat landscape.

These release notes accompany Sky ATP. They describe known behavior in the hardware and software.

### Recommended Software Version

See the [Sky Advanced Threat Prevention Supported Platforms Guide](#) for information supported software versions.

### New and Changed Features

---

This section describes the new features and enhancements to existing features in Junos OS Release 15.1X49-D80 for Sky ATP.

For the latest updates and enhancements to the cloud portal, see the [New Features](#) document.

- [E-Mail Attachments on page 2](#)
- [SSL Proxy for Server Protection on page 3](#)

### E-Mail Attachments

Starting in Junos OS Release 15.1X49-D80, e-mail management for SMTP lets enrolled SRX Series devices transparently submit potentially malicious e-mail attachments to the cloud for inspection. Once an attachment is evaluated, Sky ATP assigns the file a threat score from 0 through 10 with 10 being the most malicious. In addition, e-mails are

checked against administrator-configured blacklists and whitelists. If an e-mail matches the blacklist, it is considered to be malicious and is handled the same way as an e-mail with a malicious attachment.

[See [Email Management Overview](#).]

## SSL Proxy for Server Protection

SSL proxy is a transparent proxy that performs SSL encryption and decryption between the client and the server. Starting in Junos OS Release 15.1X49-D80, the proxy model implementation for server protection (often called *reverse proxy*) is based on existing SSL plug-ins to provide improved handshaking and support for more protocol versions.

[See [Configuring Reverse Proxy](#).]

## Changes in Behavior and Syntax

---

This section lists the changes in behavior of Sky ATP features and in Junos OS Release 15.1X49-D80 for Sky ATP.

- [HA Failover and Security Intelligence Daemon on page 3](#)
- [Match Condition on page 4](#)

## HA Failover and Security Intelligence Daemon

Starting with Junos OS Release 15.1X49-D80, HA failover is not supported when the security intelligence daemon is disabled (**set system processes security-intelligence disable**.)

## Match Condition

Starting in Junos OS Release 15.1X49-D80, the **match-then** condition has been deprecated from the Sky ATP policy configuration.

Prior to Junos OS Release 15.1X49-D80	Junos OS Release 15.1X49-D80 and later
<pre> policy po1 {   inspection-profile insp_profile1;   match { # Deprecated     application HTTP;     verdict-threshold 8;   }   then { # Deprecated     action block;     notification log;   }   default-notification {     log;   }   whitelist-notification {     log;   }   blacklist-notification {     log;   }   fallback-options {     action permit;     notification log;   } } </pre>	<pre> policy po1 {   http {     inspection-profile default_profile;     action block;   }   verdict-threshold 8;   fallback-options {     action permit;   }   default-notification {     log;   }   whitelist-notification {     log;   }   blacklist-notification {     log;   }   default-notification {     fallback-options {       action permit;     }   } } </pre>

Existing policies with the **match-then** condition are supported, but you can no longer create policies with those parameters.

## Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D80 for Sky ATP.

- After you change the revocation configuration of a CA profile, the change cannot be populated to the SSL-I's revocation check. We recommend you change the SSL-I configuration to **enable** or disable CRL checking instead of using a ca-profile configuration. [PR 1143462]
- When in HA mode, if you disable and then reenabling CRL checking of certificate validity, the system does not reenabling CRL checking. You must reboot the SRX1500 Services Gateway before CRL checking is again enabled. [PR 1144280]
- If you select the Permit action in the **Configure > Email Management > SMTP** window, e-mails with attachments are sent directly to the recipients while the attachments are sent to the cloud for analysis. If system constraints, such as memory issues, cloud connectivity issues, etc., occur while the attachment is sent to the cloud, the fallback condition is supposed to be used. However, in this case, the Permit action overrides

the fallback action. For example, if your fallback condition is Block, the Permit action as configured in the Web GUI is used. [PR 1239650]

- A file submission timeout can occur on the SRX Series device when the following conditions are present:
  - The advanced anti-malware service (AAMW) is enabled.
  - SMTP or SMTPS is configured in the AAMW policy.
  - The fallback action is permit.
  - Long network latency exists between the SRX Series device and the Sky ATP cloud service.

Under these circumstances, the e-mail remains in the sender's Outlook outbox and the recipient never receives the e-mail.

As a workaround, try to resolve the long latency issue between the SRX Series device and the Sky ATP cloud service. If this is not possible, increase the server timeout setting in the recipient's Outlook. [1254088]

- When the AAMW service is enabled and SMTP inspection is configured in the AAMW policy, SMTP e-mails encoded with the uuencode mechanism cannot be decoded or identified and as such are not inspected by the Sky ATP cloud for malware. [1236721]
- There is a small chance that the AAMW daemon core dumps under the following conditions. The AAMW daemon will automatically recover.
  - The AAMW service is enabled on the SRX Series device.
  - The SRX Series device is enrolled with Sky ATP.
  - **traceoption** is enabled with either the **flag daemon** or **flag all** option (for example, **set services advanced-anti-malware traceoptions flag daemon** or **set services advanced-anti-malware traceoptions flag all**).
  - The user continues to commit configuration changes in AAMW. [1261881]
- AAMW sessions will always use the AAMW parameters configured at the time the session was establishment. Configuration changes will not retroactively affect already established sessions. For example, a session established when the verdict threshold is 5 will always have 5 as the threshold even if the verdict threshold changes to other values during that session's lifetime.
- File submission from the vSRX to the Sky ATP cloud does not work due to an identity issue. This issue does not affect the SRX Series hardware. [1288287]

## 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 <http://www.juniper.net/techpubs/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 <http://www.juniper.net/techpubs/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 <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: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- 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://tools.juniper.net/SerialNumberEntitlementSearch/>

## 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>.

## Revision History

---

March 2017—Revision 1—Sky Advanced Threat Prevention

Copyright © 2017 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.