

# Sky ATP

---

## Juniper Sky Advanced Threat Prevention Administration Guide

Published  
2020-07-01

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.

*Sky ATP Juniper Sky Advanced Threat Prevention Administration Guide*  
Copyright © 2020 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 | x**

Documentation and Release Notes | x

Documentation Conventions | x

Documentation Feedback | **xiii**

Requesting Technical Support | **xiii**

Self-Help Online Tools and Resources | **xiv**

Creating a Service Request with JTAC | **xiv**

1

## **Overview and Installation**

### **Juniper Sky Advanced Threat Prevention Overview | 2**

Juniper Sky Advanced Threat Prevention | 2

About Juniper Sky Advanced Threat Prevention | 2

Juniper Sky ATP Features | 4

How the SRX Series Device Remediates Traffic | 6

Juniper Sky ATP Use Cases | 7

Licensing | 8

How is Malware Analyzed and Detected? | 9

Analyzing and Detecting Malware | 9

Cache Lookup | 10

Antivirus Scan | 10

Static Analysis | 10

Dynamic Analysis | 11

Machine Learning Algorithm | 11

Threat Levels | 11

Licensing | 12

About Policy Enforcer | 12

Policy Enforcer | 12

## **Install Juniper Sky Advanced Threat Prevention | 15**

Juniper Sky Advanced Threat Prevention Installation Overview | 15

Managing the Juniper Sky Advanced Threat Prevention License | 15

Obtaining the Premium License Key | 16

License Management and SRX Series Devices | 17

Juniper Sky ATP Premium Evaluation License for vSRX | 17

License Management and vSRX Deployments | 17

High Availability | 19

Registering a Juniper Sky Advanced Threat Prevention Account | 20

Downloading and Running the Juniper Sky Advanced Threat Prevention Script | 24

2

## **The Web Portal and Enrolling SRX Series Devices**

### **The Juniper Sky ATP Web Portal | 31**

Juniper Sky Advanced Threat Prevention Configuration Overview | 31

Juniper Sky Advanced Threat Prevention Web UI Overview | 34

Accessing the Web UI | 34

Dashboard Overview | 37

Reset Password | 38

Recover Realm Name | 40

### **Enroll SRX Series Devices | 43**

Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention | 43

Enrolling an SRX Series Device without the Juniper Sky ATP Web Portal | 47

Removing an SRX Series Device From Juniper Sky Advanced Threat Prevention | 49

Searching for SRX Series Devices Within Juniper Sky Advanced Threat Prevention | 50

Juniper Sky Advanced Threat Prevention RMA Process | 53

Device Information | 53

Cloud Feeds for Juniper Sky Advanced Threat Prevention: More Information | 54

## Configure

### Whitelists and Blacklists | 57

Whitelist and Blacklist Overview | 57

Creating Whitelists and Blacklists | 59

### Email Scanning: Juniper Sky ATP | 65

Email Management Overview | 65

Email Management: Configure SMTP | 67

Email Management: Configure IMAP | 70

### Email Scanning: SRX Series Device | 74

Configuring the SMTP Email Management Policy on the SRX Series Device | 74

Configuring the IMAP Email Management Policy on the SRX Series Device | 80

Configuring Reverse Proxy on the SRX Series Device | 88

### File Inspection Profiles | 92

File Inspection Profiles Overview | 92

Creating File Inspection Profiles | 94

### Adaptive Threat Profiling | 97

Adaptive Threat Profiling Overview | 97

Overview | 97

Configure Adaptive Threat Profiling | 99

Deploy Adaptive Threat Profiling | 101

Use Case Examples | 103

Threat Detection Use Case | 103

Asset Classification Use Case | 107

Create an Adaptive Threat Profiling Feed | 108

### Third Party Threat Feeds | 110

Enabling Third Party Threat Feeds | 110

## **Global Configurations | 116**

Global Configuration for Infected Hosts | 116

Configuring Threat Intelligence Sharing | 119

Configuring Trusted Proxy Servers | 121

Realm Overview | 122

Realms and Tenant Systems | 122

Configuration Overview | 123

SRX Series and Tenant System Enrollment | 123

Realm Management | 124

Tenant Systems: Security-Intelligence and Anti-Malware Policies | 126

Tenant System Support for SecIntel Feeds | 126

Tenant System Support for AAMW | 127

Security Profile CLI | 129

## 4

## **Monitor and Take Action**

### **Reports | 131**

Reports Overview | 131

Configure Report Definitions | 135

### **Hosts | 137**

Hosts Overview | 137

Host Details | 140

### **Identifying Infected Hosts | 142**

Compromised Hosts: More Information | 142

About Block Drop and Block Close | 146

Host Details | 147

Automatic Lowering of Host Threat Level or Removal from Infected Hosts Feed | 148

Configuring the SRX Series Devices to Block Infected Hosts | 149

### **Command and Control Servers | 153**

Command and Control Servers Overview | 153

Command and Control Server Details | 154

## **Identify Hosts Communicating with Command and Control Servers | 158**

Command and Control Servers: More Information | 158

Configuring the SRX Series Device to Block Outbound Requests to a C&C Host | 161

## **File Scanning | 164**

HTTP File Download Overview | 164

HTTP File Download Details | 166

File Summary | 167

HTTP Downloads | 168

Sample STIX Report | 169

Manual Scanning Overview | 169

File Scanning Limits | 171

## **Email Scanning | 173**

Email Attachments Scanning Overview | 173

Email Attachments Scanning Details | 174

File Summary | 176

SMTP Quarantine Overview: Blocked Emails | 177

IMAP Block Overview | 179

## **Telemetry | 181**

Telemetry Overview | 181

Telemetry Details | 183

## **Encrypted Traffic Analysis | 185**

Encrypted Traffic Analysis Overview | 185

Encrypted Traffic Analysis and Detection | 186

Workflow | 187

Configurations on SRX Series Devices | 188

Encrypted Traffic Analysis Details | 189

## 5

**Policies on the SRX Series Device****Configure Juniper Sky ATP Policies on the SRX Series Device | 193**

Juniper Sky Advanced Threat Prevention Policy Overview | 193

Enabling Juniper Sky ATP for Encrypted HTTPS Connections | 196

Example: Configuring a Juniper Sky Advanced Threat Prevention Policy Using the CLI | 197

Unified Policies | 202

Explicit Web Proxy Support | 204

**Configure IP-Based Geolocations on the SRX Series Device | 206**

Geolocation IPs and Juniper Sky Advanced Threat Prevention | 206

Configuring Juniper Sky Advanced Threat Prevention With Geolocation IP | 207

## 6

**Administration****Juniper Sky ATP Administration | 210**

Modifying My Profile | 210

Creating and Editing User Profiles | 211

Application Tokens Overview | 213

Creating Application Tokens | 213

Multi-Factor Authentication Overview | 215

Configure Multi-Factor Authentication for Administrators | 215

Enable Multi-Factor Authentication | 216

Verification Codes for Multi-Factor Authentication: Mobile SMS | 217

Verification Codes for Multi-Factor Authentication: Email | 217

Unlock a User | 218

## 7

**Troubleshoot****Troubleshooting Topics | 220**

Juniper Sky Advanced Threat Prevention Troubleshooting Overview | 220

Troubleshooting Juniper Sky Advanced Threat Prevention: Checking DNS and Routing Configurations | 221

Troubleshooting Juniper Sky Advanced Threat Prevention: Checking Certificates | 224

Troubleshooting Juniper Sky Advanced Threat Prevention: Checking the Routing Engine Status | 226

request services advanced-anti-malware data-connection | 228

request services advanced-anti-malware diagnostic | 230



Troubleshooting Juniper Sky Advanced Threat Prevention: Checking the application-identification License | **234**

Viewing Juniper Sky Advanced Threat Prevention System Log Messages | **235**

Configuring traceoptions | **236**

Viewing the traceoptions Log File | **238**

Turning Off traceoptions | **238**

Juniper Sky Advanced Threat Prevention Dashboard Reports Not Displaying | **239**

Juniper Sky Advanced Threat Prevention RMA Process | **240**

8

## **More Documentation**

**Sky ATP Tech Library Page Links | 242**

Links to Documentation on Juniper.net | **242**

# About the Documentation

## IN THIS SECTION

- Documentation and Release Notes | x
- Documentation Conventions | x
- Documentation Feedback | xiii
- Requesting Technical Support | xiii

Use this guide to configure, monitor, and manage Juniper Sky ATP features to protect all hosts in your network against evolving security threats.

## 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 xi](#) 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 xi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<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@# <b>set system domain-name</b> <i>domain-name</i>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit <b>protocols ospf area area-id</b>] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub &lt;default-metric <i>metric</i>&gt;;</b>
(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.	<b>broadcast   multicast</b>  <b>(<i>string1</i>   <i>string2</i>   <i>string3</i>)</b>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ <i>community-ids</i> ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

---

**GUI Conventions**


---

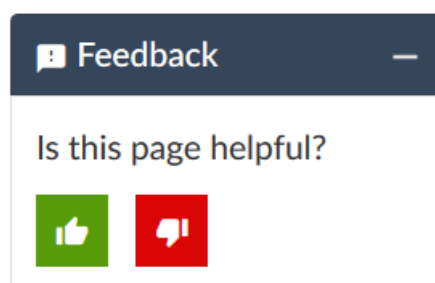
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## 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](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 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/>.

# 1

PART

## Overview and Installation

---

[Juniper Sky Advanced Threat Prevention Overview | 2](#)

[Install Juniper Sky Advanced Threat Prevention | 15](#)

---

# Juniper Sky Advanced Threat Prevention Overview

## IN THIS CHAPTER

- Juniper Sky Advanced Threat Prevention | 2
- How is Malware Analyzed and Detected? | 9
- About Policy Enforcer | 12

## Juniper Sky Advanced Threat Prevention

### IN THIS SECTION

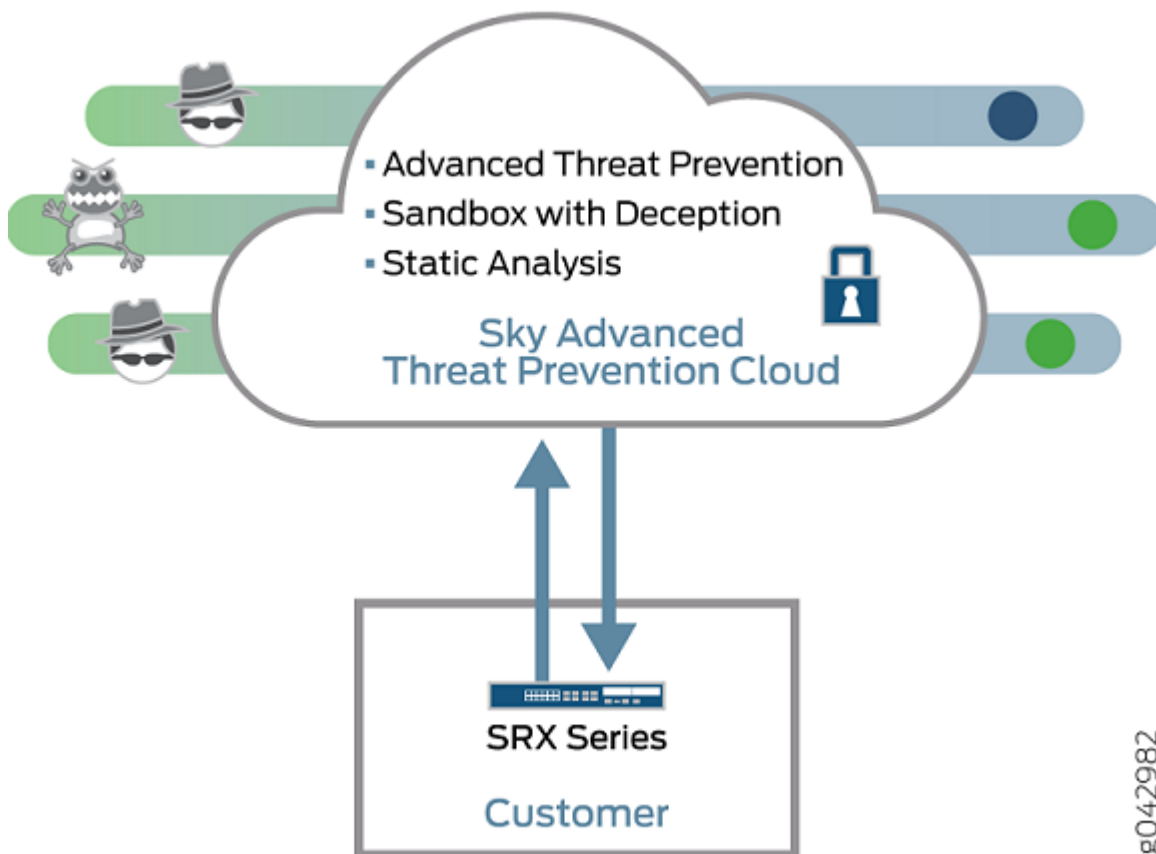
- About Juniper Sky Advanced Threat Prevention | 2
- Juniper Sky ATP Features | 4
- How the SRX Series Device Remediate Traffic | 6
- Juniper Sky ATP Use Cases | 7
- Licensing | 8

### About Juniper Sky Advanced Threat Prevention

Juniper Sky™ Advanced Threat Prevention (Juniper Sky ATP) is a security framework that protects all hosts in your network against evolving security threats by employing cloud-based threat detection software with a next-generation firewall system. See [Figure 1 on page 3](#).



Figure 1: Juniper Sky ATP Overview



Juniper Sky ATP protects your network by performing the following tasks:

- The SRX Series device extracts potentially malicious objects and files and sends them to the cloud for analysis.
- Known malicious files are quickly identified and dropped before they can infect a host.
- Multiple techniques identify new malware, adding it to the known list of malware.
- Correlation between newly identified malware and known Command and Control (C&C) sites aids analysis.
- The SRX Series device blocks known malicious file downloads and outbound C&C traffic.

Juniper Sky ATP supports the following modes:

- Layer 3 mode
- Tap mode

- Transparent mode using MAC address. For more information, see [Transparent mode on SRX Series devices](#).
- Secure wire mode (high-level transparent mode using the interface to directly passing traffic, not by MAC address.) For more information, see [Understanding Secure Wire](#).

## Juniper Sky ATP Features

Juniper Sky ATP is a cloud-based solution. Cloud environments are flexible and scalable, and a shared environment ensures that everyone benefits from new threat intelligence in near real-time. Your sensitive data is secured even though it is in a cloud shared environment. Security analysts can update their defense when new attack techniques are discovered and distribute the threat intelligence with very little delay.

In addition, Juniper Sky ATP offers the following features:

- Integrated with the SRX Series device to simplify deployment and enhance the anti-threat capabilities of the firewall.
- Delivers protection against “zero-day” threats using a combination of tools to provide robust coverage against sophisticated, evasive threats.
- Checks inbound and outbound traffic with policy enhancements that allow users to stop malware, quarantine infected systems, prevent data exfiltration, and disrupt lateral movement.
- High availability to provide uninterrupted service.
- Scalable to handle increasing loads that require more computing resources, increased network bandwidth to receive more customer submissions, and a large storage for malware.
- Provides deep inspection, actionable reporting, and inline malware blocking.
- APIs for C&C feeds, whitelist and blacklist operations, and file submission. See the [Threat Intelligence Open API Setup Guide](#) for more information.

[Figure 2 on page 5](#) lists the Juniper Sky ATP components.

Figure 2: Juniper Sky ATP Components

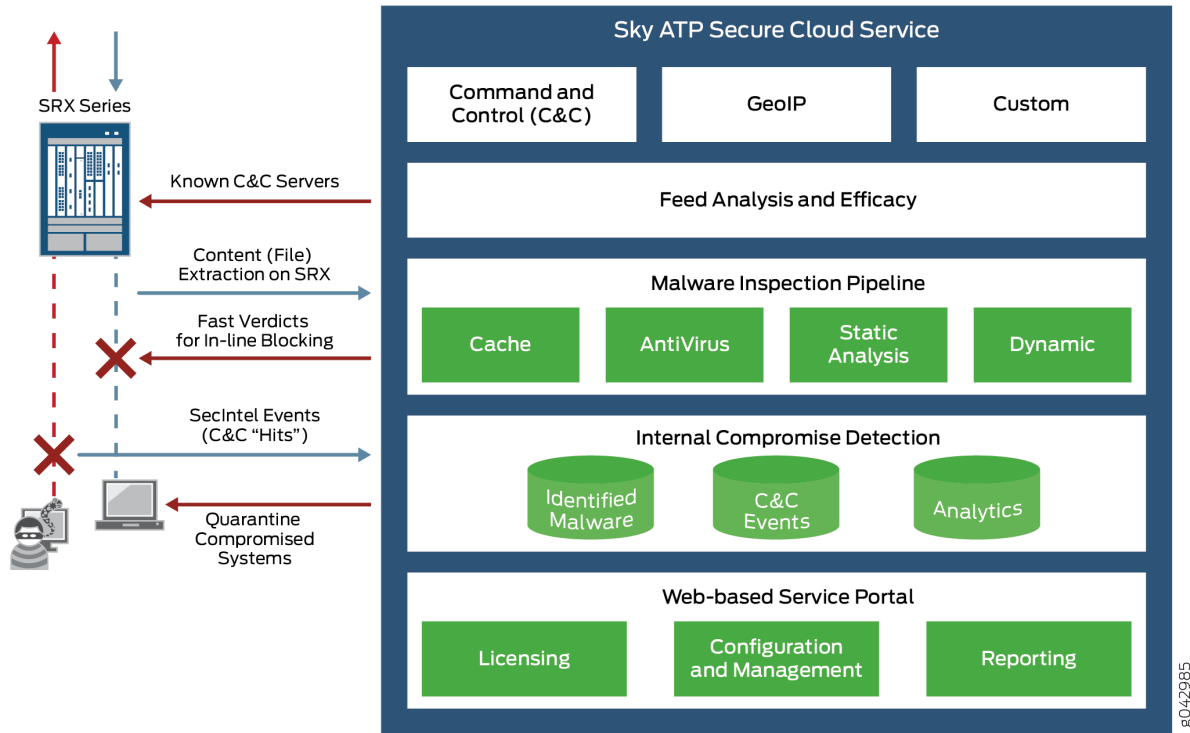


Table 3 on page 5 briefly describes each Juniper Sky ATP component's operation.

Table 3: Juniper Sky ATP Components

Component	Operation
Command and control (C&C) cloud feeds	C&C feeds are essentially a list of servers that are known command and control for botnets. The list also includes servers that are known sources for malware downloads.
GeolP cloud feeds	GeolP feeds is an up-to-date mapping of IP addresses to geographical regions. This gives you the ability to filter traffic to and from specific geographies in the world.
Infected host cloud feeds	Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or other exhibit other symptoms.
Whitelists, blacklists and custom cloud feeds	A whitelist is simply a list of known IP addresses that you trust and a blacklist is a list that you do not trust.  <b>NOTE:</b> Custom feeds are not supported in this release.

**Table 3: Juniper Sky ATP Components (continued)**

Component	Operation
SRX Series device	Submits extracted file content for analysis and detected C&C hits inside the customer network.  Performs inline blocking based on verdicts from the analysis cluster.
Malware inspection pipeline	Performs malware analysis and threat detection.
Internal compromise detection	Inspects files, metadata, and other information.
Service portal (Web UI)	Graphics interface displaying information about detected threats inside the customer network.  Configuration management tool where customers can fine-tune which file categories can be submitted into the cloud for processing.

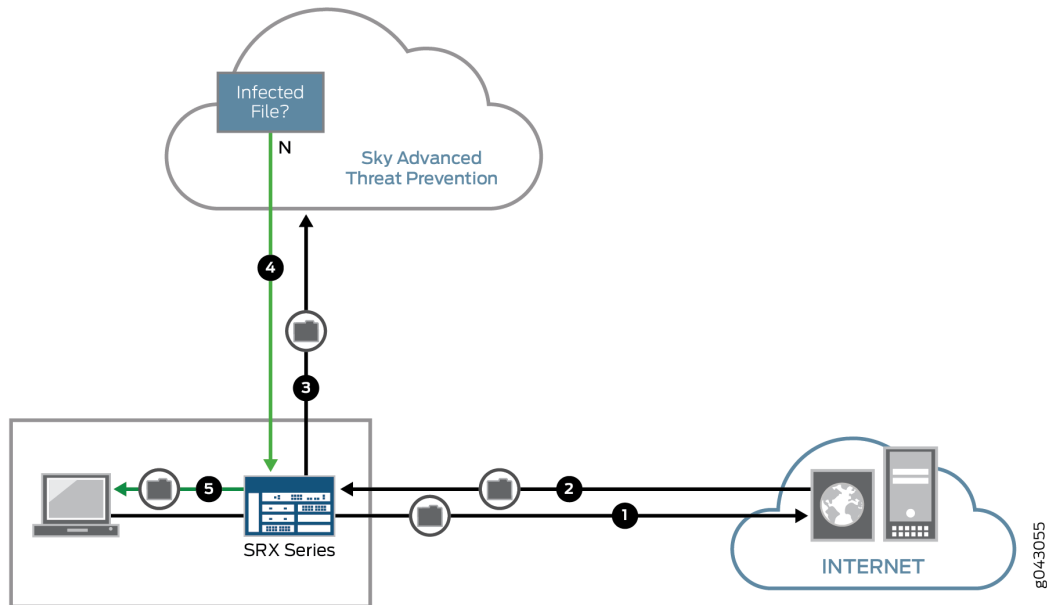
### How the SRX Series Device Remediates Traffic

The SRX Series devices use intelligence provided by Juniper Sky ATP to remediate malicious content through the use of security policies. If configured, security policies block that content before it is delivered to the destination address.

For inbound traffic, security policies on the SRX Series device look for specific types of files, like .exe files, to inspect. When one is encountered, the security policy sends the file to the Juniper Sky ATP cloud for inspection. The SRX Series device holds the last few KB of the file from the destination client while Juniper Sky ATP checks if this file has already been analyzed. If so, a verdict is returned and the file is either sent to the client or blocked depending on the file's threat level and the user-defined policy in place. If the cloud has not inspected this file before, the file is sent to the client while Juniper Sky ATP performs an exhaustive analysis. If the file's threat level indicates malware (and depending on the user-defined configurations) the client system is marked as an infected host and blocked from outbound traffic. For more information, see [“How is Malware Analyzed and Detected?” on page 9](#).

[Figure 3 on page 7](#) shows an example flow of a client requesting a file download with Juniper Sky ATP.

Figure 3: Inspecting Inbound Files for Malware



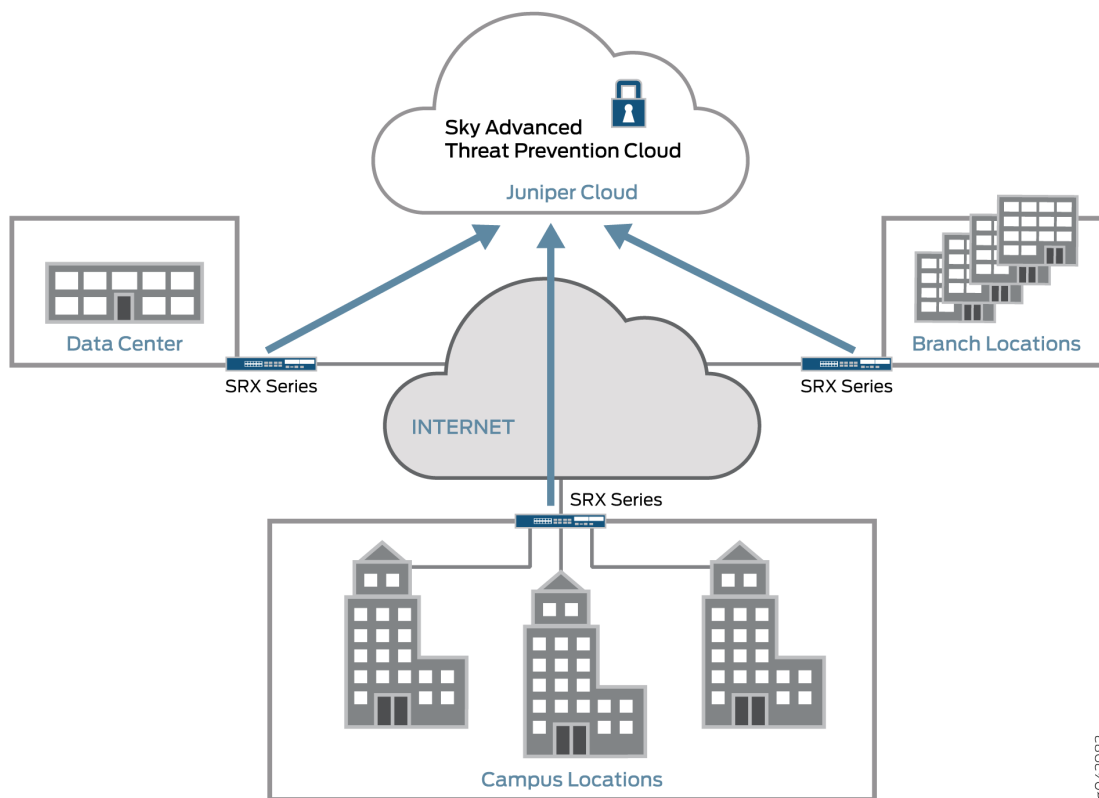
Step	Description
1	A client system behind an SRX Series devices requests a file download from the Internet. The SRX Series device forwards that request to the appropriate server.
2	The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must be performed.
3	The downloaded file type is on the list of files that must be inspected and is sent to the cloud for analysis.
4	Juniper Sky ATP has inspected this file before and has the analysis stored in cache. In this example, the file is not malware and the verdict is sent back to the SRX Series device.
5	Based on user-defined policies and because this file is not malware, the SRX Series device sends the file to the client.

For outbound traffic, the SRX Series device monitors traffic that matches C&C feeds it receives, blocks these C&C requests, and reports them to Juniper Sky ATP. A list of infected hosts is available so that the SRX Series device can block inbound and outbound traffic.

### Juniper Sky ATP Use Cases

Juniper Sky ATP can be used anywhere in an SRX Series deployment. See [Figure 4 on page 8](#).

Figure 4: Juniper Sky ATP Use Cases



8042983

- Campus edge firewall—Juniper Sky ATP analyzes files downloaded from the Internet and protects end-user devices.
- Data center edge—Like the campus edge firewall, Juniper Sky ATP prevents infected files and application malware from running on your computers.
- Branch router—Juniper Sky ATP provides protection from split-tunneling deployments. A disadvantage of split-tunneling is that users can bypass security set in place by your company's infrastructure.

## Licensing

Juniper Sky ATP has three service levels: Free, Basic (feed only), and Premium. No license is required for the free version, but you must obtain a license for Basic and Premium levels.

To understand more about Juniper Sky ATP licenses, see [Licenses for Juniper Sky Advanced Threat Prevention \(ATP\)](#). Please refer to the [Licensing Guide](#) for general information about License Management. Please refer to the product Data Sheets for further details, or contact your Juniper Account Team or Juniper Partner.

## How is Malware Analyzed and Detected?

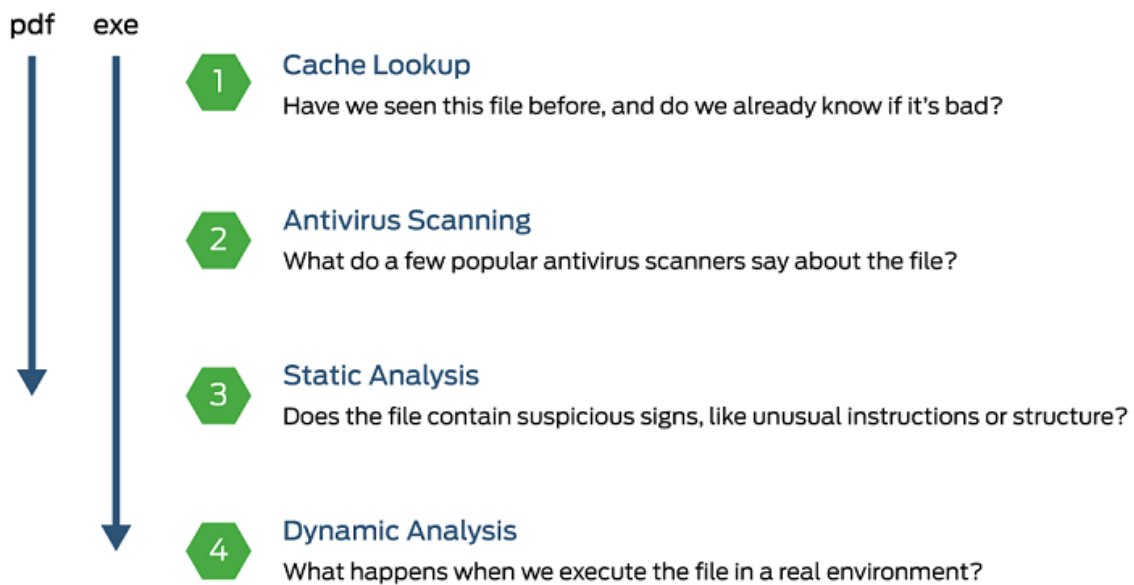
### IN THIS SECTION

- Analyzing and Detecting Malware | 9
- Cache Lookup | 10
- Antivirus Scan | 10
- Static Analysis | 10
- Dynamic Analysis | 11
- Machine Learning Algorithm | 11
- Threat Levels | 11
- Licensing | 12

### Analyzing and Detecting Malware

Juniper Sky ATP uses a pipeline approach to analyzing and detecting malware. If an analysis reveals that the file is absolutely malware, it is not necessary to continue the pipeline to further examine the malware. See [Figure 5 on page 9](#).

Figure 5: Example Juniper Sky ATP Pipeline Approach for Analyzing Malware



Each analysis technique creates a verdict number, which is combined to create a final verdict number between 1 and 10. A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

## Cache Lookup

When a file is analyzed, a file hash is generated, and the results of the analysis are stored in a database. When a file is uploaded to the Juniper Sky ATP cloud, the first step is to check whether this file has been looked at before. If it has, the stored verdict is returned to the SRX Series device and there is no need to re-analyze the file. In addition to files scanned by Juniper Sky ATP, information about common malware files is also stored to provide faster response.

Cache lookup is performed in real time. All other techniques are done offline. This means that if the cache lookup does not return a verdict, the file is sent to the client system while the Juniper Sky ATP cloud continues to examine the file using the remaining pipeline techniques. If a later analysis returns a malware verdict, then the file and host are flagged.

## Antivirus Scan

The advantage of antivirus software is its protection against a large number of potential threats, such as viruses, trojans, worms, spyware, and rootkits. The disadvantage of antivirus software is that it is always behind the malware. The virus comes first and the patch to the virus comes second. Antivirus is better at defending familiar threats and known malware than zero-day threats.

Juniper Sky ATP utilizes multiple antivirus software packages, not just one, to analyze a file. The results are then fed into the machine learning algorithm to overcome false positives and false negatives.

## Static Analysis

Static analysis examines files without actually running them. Basic static analysis is straightforward and fast, typically around 30 seconds. The following are examples of areas static analysis inspects:

- Metadata information—Name of the file, the vendor or creator of this file, and the original data the file was compiled on.
- Categories of instructions used—Is the file modifying the Windows registry? Is it touching disk I/O APIs?
- File entropy—How random is the file? A common technique for malware is to encrypt portions of the code and then decrypt it during runtime. A lot of encryption is a strong indication a this file is malware.

The output of the static analysis is fed into the machine learning algorithm to improve the verdict accuracy.



## Dynamic Analysis

The majority of the time spent inspecting a file is in dynamic analysis. With dynamic analysis, often called *sandboxing*, a file is studied as it is executed in a secure environment. During this analysis, an operating system environment is set up, typically in a virtual machine, and tools are started to monitor all activity. The file is uploaded to this environment and is allowed to run for several minutes. Once the allotted time has passed, the record of activity is downloaded and passed to the machine learning algorithm to generate a verdict.

Sophisticated malware can detect a sandbox environment due to its lack of human interaction, such as mouse movement. Juniper Sky ATP uses a number of *deception techniques* to trick the malware into determining this is a real user environment. For example, Juniper Sky ATP can:

- Generate a realistic pattern of user interaction such as mouse movement, simulating keystrokes, and installing and launching common software packages.
- Create fake high-value targets in the client, such as stored credentials, user files, and a realistic network with Internet access.
- Create vulnerable areas in the operating system.

Deception techniques by themselves greatly boost the detection rate while reducing false positives. They also boost the detection rate of the sandbox the file is running in because they get the malware to perform more activity. The more the file runs the more data is obtained to detect whether it is malware.

## Machine Learning Algorithm

Juniper Sky ATP uses its own proprietary implementation of machine learning to assist in analysis. Machine learning recognizes patterns and correlates information for improved file analysis. The machine learning algorithm is programmed with features from thousands of malware samples and thousands of goodware samples. It learns what malware looks like, and is regularly re-programmed to get smarter as threats evolve.

## Threat Levels

Juniper Sky ATP assigns a number between 0-10 to indicate the threat level of files scanned for malware and the threat level for infected hosts. See [Table 4 on page 11](#).

Table 4: Threat Level Definitions

Threat Level	Definition
0	Clean; no action is required.
1 - 3	Low threat level.
4 - 6	Medium threat level.

Table 4: Threat Level Definitions (*continued*)

Threat Level	Definition
7 -10	High threat level.

For more information on threat levels, see the Juniper Sky ATP Web UI online help.

## Licensing

Juniper Sky ATP has three service levels: Free, Basic (feed only), and Premium. No license is required for the free version, but you must obtain a license for Basic and Premium levels.

To understand more about Juniper Sky ATP licenses, see [Licenses for Juniper Sky Advanced Threat Prevention \(ATP\)](#). Please refer to the [Licensing Guide](#) for general information about License Management. Please refer to the product Data Sheets for further details, or contact your Juniper Account Team or Juniper Partner.

## RELATED DOCUMENTATION

[Juniper Sky Advanced Threat Prevention | 2](#)

[Dashboard Overview | 37](#)

## About Policy Enforcer

### IN THIS SECTION

- [Policy Enforcer | 12](#)

## Policy Enforcer

View the Policy Enforcer data sheet (This takes you out of the help center to the Juniper web site): <https://www.juniper.net/assets/fr/fr/local/pdf/datasheets/1000602-en.pdf>

Policy Enforcer 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.

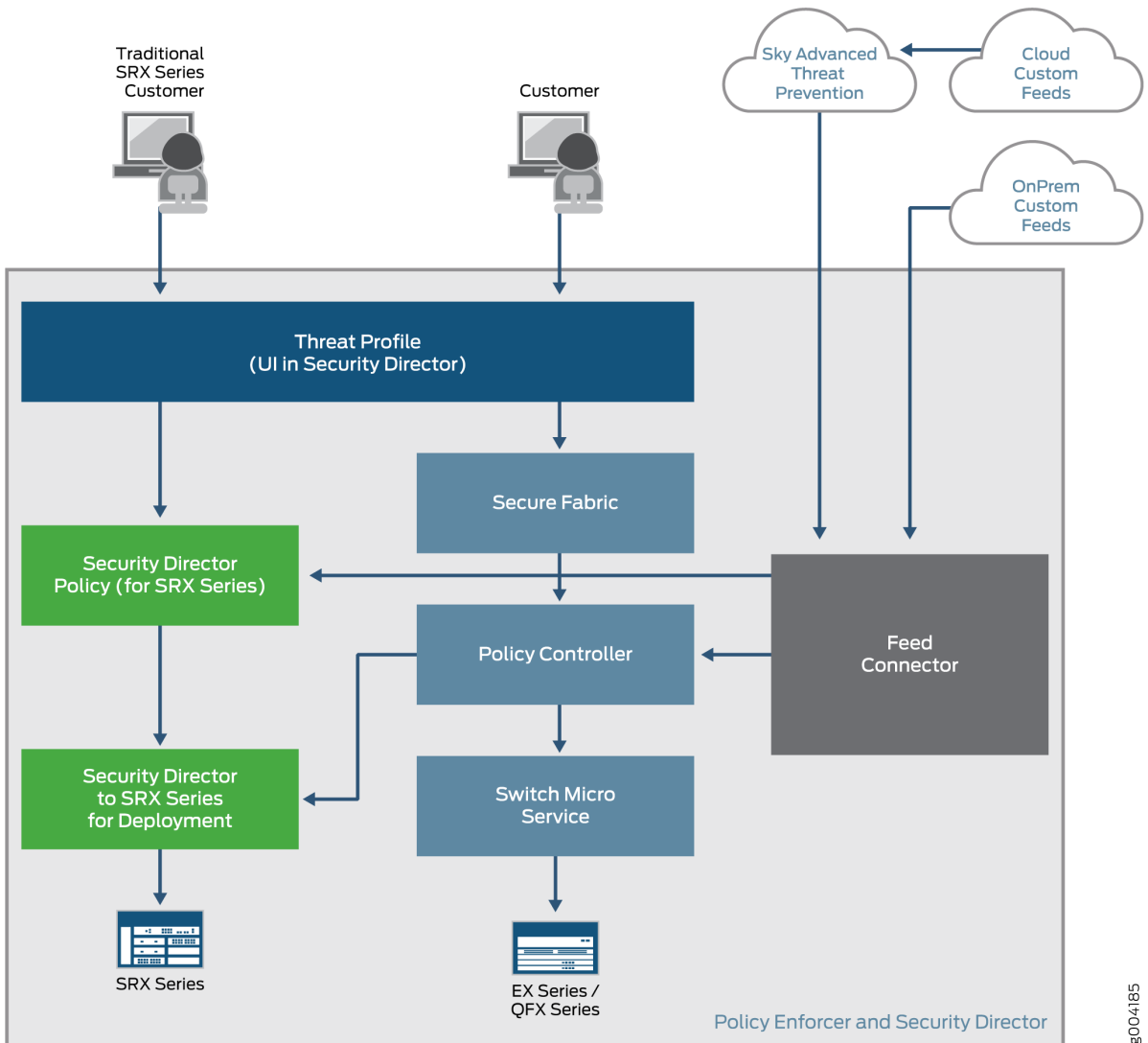
It also automates the enforcement of security policies across the network and quarantines infected endpoints to prevent threats across firewalls and switches. It works with cloud-based Juniper Sky Advanced Threat Prevention (Juniper Sky ATP) to protect both perimeter-oriented threats as well as threats within the network. For example, if a user downloads a file from the Internet and that file passes through an SRX firewall, the file can be sent to the Juniper Sky ATP cloud for malware inspection (depending on your configuration settings.) If the file is determined to be malware, Policy Enforcer identifies the IP address and MAC address of the host that downloaded the file. Based on a user-defined policy, that host can be put into a quarantine VLAN or blocked from accessing the Internet.

Policy Enforcer provides the following:

- Pervasive Security—Combine security features and intelligence from devices across your network, including switches, routers, 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, it can also act as a sensor, providing visibility for intra- and inter-network communications.
- User Intent-Based Policies—Create 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—Gather threat information from multiple locations and devices, both physical and virtual, as well as third party solutions.

[Figure 6 on page 14](#) illustrates the flow diagram of Policy Enforcer over a traditional SRX configuration.

Figure 6: Comparing Traditional SRX Customers to Policy Enforcer Customers



RELATED DOCUMENTATION

[Hosts Overview | 137](#)

[Host Details | 140](#)

[Dashboard Overview | 37](#)

# Install Juniper Sky Advanced Threat Prevention

## IN THIS CHAPTER

- Juniper Sky Advanced Threat Prevention Installation Overview | 15
- Managing the Juniper Sky Advanced Threat Prevention License | 15
- Registering a Juniper Sky Advanced Threat Prevention Account | 20
- Downloading and Running the Juniper Sky Advanced Threat Prevention Script | 24

## Juniper Sky Advanced Threat Prevention Installation Overview

Although Juniper Sky ATP is a free add-on to an SRX Series device, you must still enable it prior to using it. To enable Juniper Sky ATP, perform the following tasks:

1. (Optional) Obtain a Juniper Sky ATP premium license. See [Licenses for Juniper Sky Advanced Threat Prevention \(ATP\)](#). This link takes you to the Juniper Licensing Guide.
2. Register an account on the Juniper Sky ATP cloud Web portal. See “[Registering a Juniper Sky Advanced Threat Prevention Account](#)” on page 20.
3. Download and run the Juniper Sky ATP script on your SRX Series device. See “[Downloading and Running the Juniper Sky Advanced Threat Prevention Script](#)” on page 24.

## Managing the Juniper Sky Advanced Threat Prevention License

### IN THIS SECTION

- Obtaining the Premium License Key | 16
- License Management and SRX Series Devices | 17
- Juniper Sky ATP Premium Evaluation License for vSRX | 17

- License Management and vSRX Deployments | 17
- High Availability | 19

This topic describes how to install the Juniper Sky ATP premium license onto your SRX Series devices and vSRX deployments. You do not need to install the Juniper Sky ATP free license as these are included your base software. Note that the free license has a limited feature set (see *Juniper Sky Advanced Threat Prevention License Types* and *Sky Advanced Threat Prevention File Limitations*).

When installing the license key, you must use the license that is specific your device type. For example, the Juniper Sky ATP premium license available for the SRX Series device cannot be used on vSRX deployments.

## Obtaining the Premium License Key

The Juniper Sky ATP premium license can be found on the Juniper Networks product price list. The procedure for obtaining the premium license entitlement is the same as for all other Juniper Network products. The following steps provide an overview.

1. Contact your local sales office or Juniper Networks partner to place an order for the Juniper Sky ATP premium license.

After your order is complete, an authorization code is e-mailed to you. An authorization code is a unique 16-digit alphanumeric used in conjunction with your device serial number to generate a premium license entitlement.

2. (SRX Series devices only) Use the **show chassis hardware** CLI command to find the serial number of the SRX Series devices that are to be tied to the Juniper Sky ATP premium license.

```
[edit]
root@SRX# run show chassis hardware
Hardware inventory:
Item                Version  Part number  Serial number  Description
Chassis
Midplane            REV 09   750-058562   ACMH1590      SRX1500
Pseudo CB 0
Routing Engine 0    BUILTIN  BUILTIN      SRX Routing Engine
FPC 0               REV 08   711-053832   ACMG3280      FEB
PIC 0               BUILTIN  BUILTIN      12x1G-T-4x1G-SFP-4x10G
```

Look for the serial number associated with the chassis item. In the above example, the serial number is **CM1915AK0326**.

3. Open a browser window and go to <https://license.juniper.net>.
4. Click **Login to Generate License Keys** and follow the instructions.

**NOTE:** You must have a valid Juniper Networks Customer Support Center (CSC) account to log in.

## License Management and SRX Series Devices

Unlike other Juniper Networks products, Juniper Sky ATP does not require you to install a license key onto your SRX Series device. Instead, your entitlement for a specific serial number is automatically transferred to the cloud server when you generate your license key. It may take up to 24 hours for your activation to be updated in the Juniper Sky ATP cloud server.

### Juniper Sky ATP Premium Evaluation License for vSRX

The 30-day Juniper Sky ATP countdown premium evaluation license allows you to protect your network from advanced threats with Juniper Sky ATP. The license allows you to use Juniper Sky ATP premium features for 30-days without having to install a license key. After the trial license expires, the connection to the Juniper Sky ATP cloud is broken and you will no longer be able to use any Juniper Sky ATP features.

Instructions for downloading the trial license are here: <https://www.juniper.net/us/en/dm/free-vsrx-trial/>.

**NOTE:** The 30-day trial license period begins on the day you install the evaluation license.

To continue using Juniper Sky ATP features after the optional 30-day period, you must purchase and install the date-based license; otherwise, the features are disabled.

After installing your trial license, set up your realm and contact information before using Juniper Sky ATP. For more information, see [Registering a Juniper Sky Advanced Threat Prevention Account](#).

## License Management and vSRX Deployments

Unlike with physical SRX Series devices, you must install Juniper Sky ATP premium licenses onto your vSRX. Installing the Juniper Sky ATP license follows the same procedure as with most standard vSRX licenses.

The following instructions describe how to install a license key from the CLI. You can also add a new license key with J-Web (see [Managing Licenses for vSRX](#).)

**NOTE:** If you are reinstalling a Juniper Sky ATP license key on your vSRX, you must first remove the existing Juniper Sky ATP license. For information on removing licenses on the vSRX, see [Managing Licenses for vSRX](#).

To install a license key from the CLI:

1. Use the **request system license add** command to manually paste the license key in the terminal.

```
user@vsrx> request system license add terminal
```

```
[Type ^D at a new line to end input,
enter blank line between each license key]

JUNOS123456  aaaaaa bbbbbb cccccc dddddd eeeeee ffffff
             cccccc bbbbbb dddddd aaaaaa ffffff aaaaaa
             aaaaaa bbbbbb cccccc dddddd eeeeee ffffff
             cccccc bbbbbb dddddd aaaaaa ffffff

JUNOS123456: successfully added
add license complete (no errors)
```

**NOTE:** You can save the license key to a file and upload the file to the vSRX file system through FTP or Secure Copy (SCP), and then use the **request system license add *file-name*** command to install the license.

2. (Optional) Use the **show system license** command to view details of the licenses.

Example of a premium license output:

```
root@host> show system license

License identifier: JUNOS123456
License version: 4
Software Serial Number: 1234567890
Customer ID: JuniperTest
```



```
Features:
  Sky ATP          - Sky ATP: Cloud Based Advanced Threat Prevention on SRX
firewalls
  date-based, 2016-07-19 17:00:00 PDT - 2016-07-30 17:00:00 PDT
```

Example of a free license output:

```
root@host> show system license

License identifier: JUNOS123456
License version: 4
Software Serial Number: 1234567890
Customer ID: JuniperTest
Features:
  Virtual Appliance - Virtual Appliance permanent
```

3. The license key is installed and activated on your vSRX.

## High Availability

Before enrolling your devices with the Juniper Sky ATP cloud, set up your HA cluster as described in your product documentation. For vSRX deployments, make sure the same license key is used on both cluster nodes. When enrolling your devices, you only need to enroll one node. The Juniper Sky ATP cloud will recognize this is an HA cluster and will automatically enroll the other node.

## Registering a Juniper Sky Advanced Threat Prevention Account

To create a Juniper Sky ATP account, you must first have a Customer Support Center (CSC) user account. For more information, see [Creating a User Account](#).

When setting up your Juniper Sky ATP account, you must come up with a realm name that uniquely identifies you and your company. For example, you can use your company name and your location, such as **Juniper-Mktg-Sunnyvale**, for your realm name. Realm names can only contain alphanumeric characters and the dash (“-”) symbol.

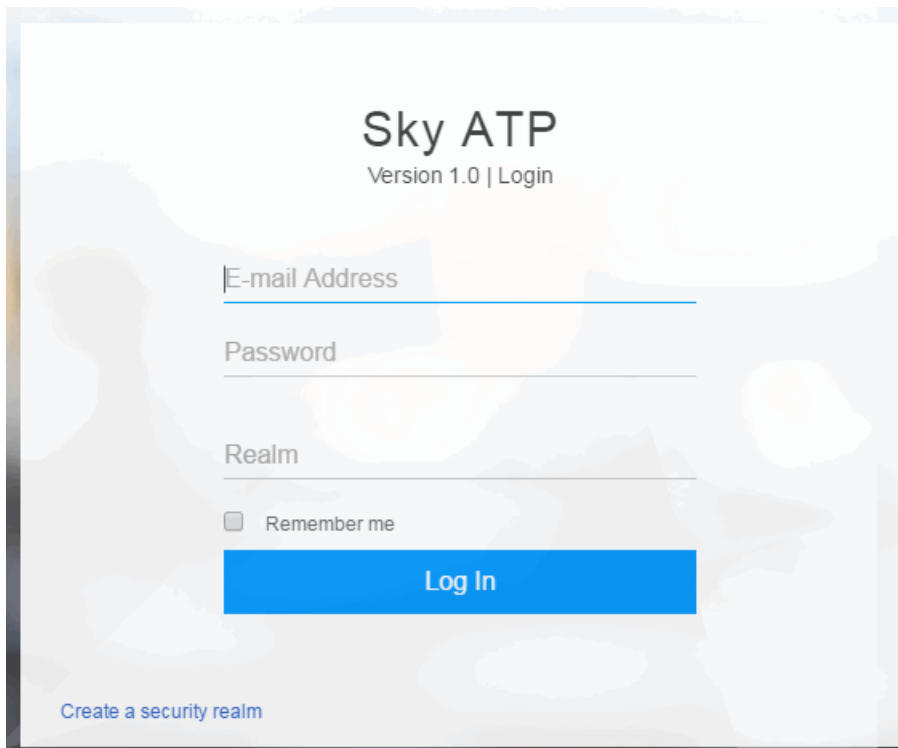
To create a Juniper Sky ATP administrator account:

1. Open a Web browser, type your location specific URL and press **Enter**. (This example is for the United States. See “[Juniper Sky Advanced Threat Prevention Web UI Overview](#)” on page 34 for all portal hostnames by location.)

**<https://amer.sky.junipersecurity.net>**

The management interface login page appears. See [Figure 7 on page 20](#).

Figure 7: Juniper Sky ATP Login



The screenshot shows the Juniper Sky ATP login interface. At the top, it says "Sky ATP" and "Version 1.0 | Login". Below this are three input fields: "E-mail Address", "Password", and "Realm". Under the "Realm" field is a checkbox labeled "Remember me". A prominent blue "Log In" button is centered below the input fields. At the bottom left of the page, there is a link that says "Create a security realm".

2. Click **Create a security realm**.

The authentication window appears. See [Figure 8 on page 21](#).

3. Enter your single sign-on (SSO) or CSC username and password and click **Next**. This is the same username and password as your CSC account.

The security realm window appears. See [Figure 8 on page 21](#).

**Figure 8: Creating Your Juniper Sky ATP Realm Name**

Sky ATP ?

1 2 3  
Realm Info Contact Info User Credentials

Version 1.0 | Create security realm

Provide your security realm with a unique name. You may want to name your realm after your division or working group. You will be unable to change this later.

Enter Security Realm Name

Company Name

Realm Description (Optional)

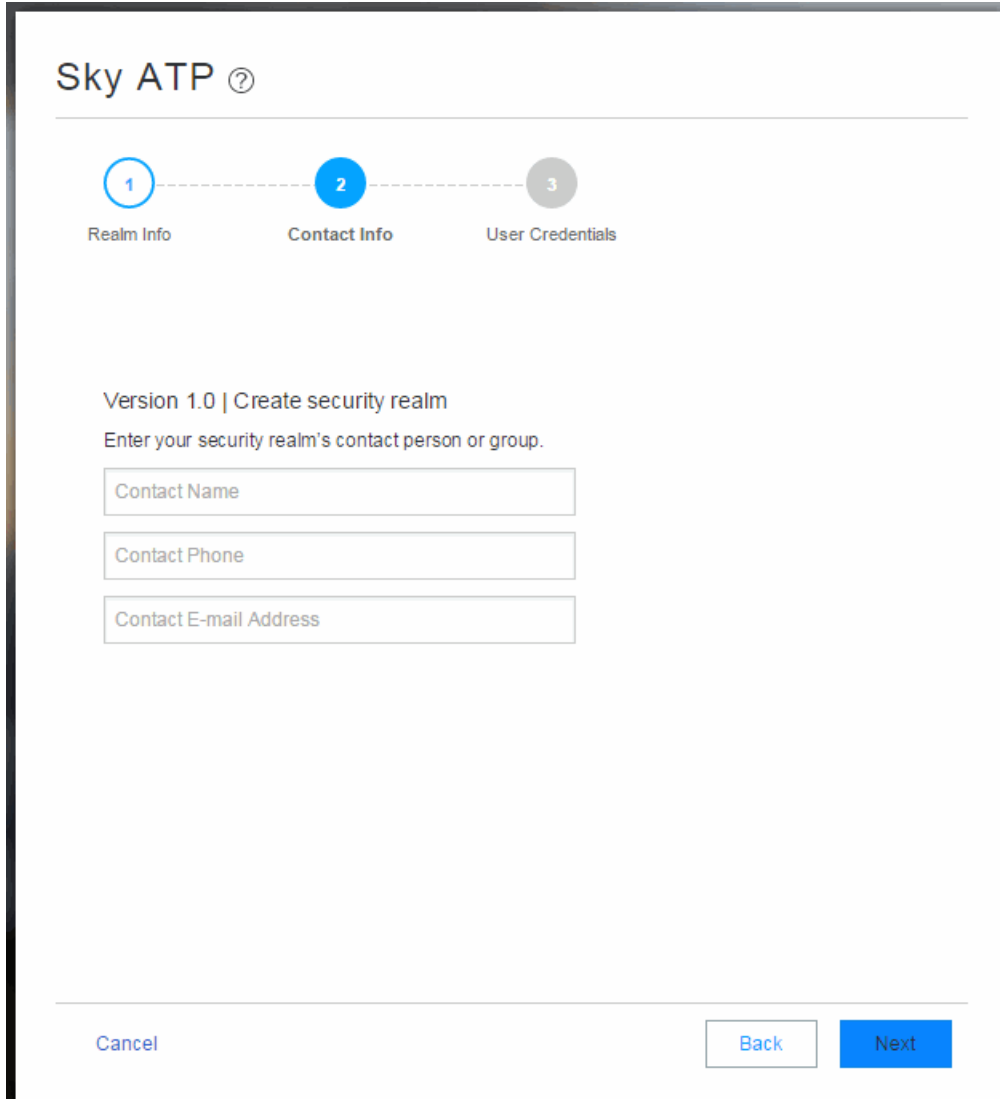
Cancel Next

4. Enter your unique realm name, company name, and optionally a description. Then press **Next**.

**NOTE:** Verify your realm name before clicking Next. Currently there is no way to delete realms through the Web UI.

The contact information window appears. See [Figure 9 on page 22](#).

Figure 9: Entering Your Juniper Sky ATP Contact Information



The screenshot shows a web interface for 'Sky ATP' with a progress indicator at the top. The progress indicator consists of three circles connected by a dashed line: the first circle is labeled '1' and 'Realm Info', the second circle is labeled '2' and 'Contact Info' (and is highlighted in blue), and the third circle is labeled '3' and 'User Credentials'. Below the progress indicator, the text reads 'Version 1.0 | Create security realm' and 'Enter your security realm's contact person or group.' There are three input fields: 'Contact Name', 'Contact Phone', and 'Contact E-mail Address'. At the bottom of the form, there are three buttons: 'Cancel', 'Back', and 'Next'.

5. Enter your contact information and click **Next**. Should Juniper Networks need to contact you, the information you enter here is used as your contact information.

The credentials window appears. See [Figure 10 on page 23](#).

Figure 10: Creating Your Juniper Sky ATP Credentials

Sky ATP ?

1 2 3  
Realm Info Contact Info User Credentials

Version 1.0 | Create username

Enter your own credentials for this security realm. This information will be unique to this specific security realm.

E-mail Address

Password

Re-enter Password

Cancel Back OK

6. Enter a valid e-mail address and password. This will be your log in information to access the Juniper Sky ATP management interface.

7. Click **Finish**.

You are automatically logged in and taken to the dashboard.

If you forget your password, you have two options:

- Create a new account on a new realm and re-enroll your devices.
- Contact Juniper Technical Support to reset your password.

## RELATED DOCUMENTATION

| [Enrolling an SRX Series Device without the Juniper Sky ATP Web Portal](#) | 47

# Downloading and Running the Juniper Sky Advanced Threat Prevention Script

The Juniper Sky ATP uses a Junos OS operation (op) script to help you configure your SRX Series device to connect to the Juniper Sky ATP cloud service. This script performs the following tasks:

- Downloads and installs certificate authority (CAs) licenses onto your SRX Series device.
- Creates local certificates and enrolls them with the cloud server.
- Performs basic Juniper Sky ATP configuration on the SRX Series device.
- Establishes a secure connection to the cloud server.

**NOTE:** Juniper Sky ATP requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) can connect to the Internet but the “to-cloud” connection should not go through the management interface, for example, fxp0. You do not need to open any ports on the SRX Series device to communicate with the cloud server. However, if you have a device in the middle, such as a firewall, then that device must have ports 8080 and 443 open.

Juniper Sky ATP requires that your SRX Series device host name contain only alphanumeric ASCII characters (a-z, A-Z, 0-9), the underscore symbol ( \_ ) and the dash symbol ( - ).

For SRX340, SRX345 and SRX500M Series devices, you must run the **set security forwarding-process enhanced-services-mode** command and reboot the device before running the op script or before running the **request services advanced-anti-malware enroll** command.

```
user@host# set security forwarding-process enhanced-services-mode
```

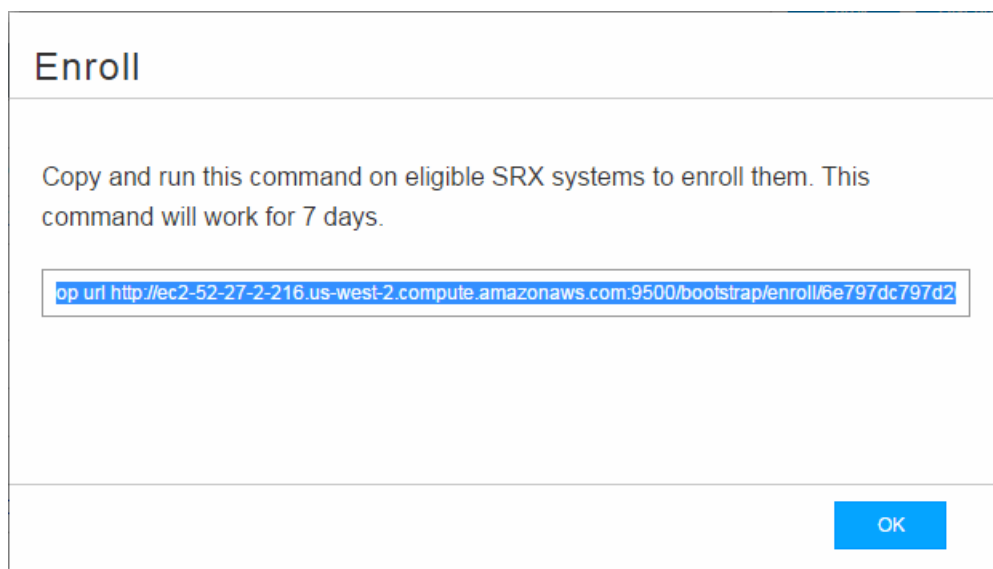
To download and run the Juniper Sky ATP script:

**NOTE:** As of Junos Release 19.3R1, there is another way to enroll the SRX series device without having to interact with the Sky ATP Web Portal. You run the “enroll” command from the SRX and it performs all the necessary enrollment steps. See [“Enrolling an SRX Series Device without the Juniper Sky ATP Web Portal” on page 47](#)

1. In the Web UI, click **Devices** and then click **Enroll**.

The Enroll window appears. See [Figure 11 on page 25](#).

**Figure 11: Enrolling Your SRX Series Device**



2. Copy the highlighted contents to your clipboard and click **OK**.

**NOTE:** When enrolling devices, Juniper Sky ATP generates a unique op script for each request. Each time you click **Enroll**, you’ll get slightly different parameters in the ops script. The screenshot above is just an example. Do not copy the above example onto your SRX device. Instead, copy and paste the output you receive from your Web UI and use that to enroll your SRX devices.

3. Paste this command into the Junos OS CLI of the SRX Series device you want to enroll with Juniper Sky ATP and press **Enter**. Your screen will look similar to the following.

```

root@mssystem> op url http://skyatp.argon.junipersecurity.net/bootstrap/
enroll/6e797dc797d26129dae46f17a7255650/jpz1qkddodlcav5g.slax
Version JUNOS Software Release [15.1-X49] is valid for bootstrapping.
Going to enroll single device for SRX1500: P1C_00000067 with hostname mssystem...
Updating Application Signature DB...
Wait for Application Signature DB download status #1...
Communicate with cloud...
Configure CA...
Request aamw-secintel-ca CA...
Load aamw-secintel-ca CA...
Request aamw-cloud-ca CA...
Load aamw-cloud-ca CA...
Retrieve CA profile aamw-ca...
Generate key pair: aamw-srx-cert...
Enroll local certificate aamw-srx-cert with CA server #1...
Configure advanced-anti-malware services...
Communicate with cloud...
Wait for aamwd connection status #1...
SRX was enrolled successfully!

```

**NOTE:** If for some reason the ops script fails, disenroll the device (see *Disenrolling an SRX Series Device from Juniper Sky Advanced Threat Prevention*) and then re-enroll it.

4. In the management interface, click **Devices**.

The SRX Series device you enrolled now appears in the table. See [Figure 12 on page 26](#).

**Figure 12: Example Enrolled SRX Series Device**

Devices / All Devices

Enrolled Devices ?

Enroll Disenroll Device Lookup

Remove

Serial Number	Host	Model Number	Tier	Last Telemetry Activity	Last Activity
<input type="checkbox"/> CM3914AK0090	pvl-forge-01	srx1500	premium	Jan 25, 2016 9:09 AM	Jan 25, 2016 9:09 AM
<input type="checkbox"/> CM3814AK0002	svlb-argon-srx	srx1500	premium	Jan 25, 2016 9:12 AM	Jan 25, 2016 9:12 AM

5. (optional) Use the **show services advanced-anti-malware status** CLI command to verify that connection is made to the cloud server from the SRX Series device. Your output will look similar to the following.



```

root@host> show services advanced-anti-malware status
Server connection status:
  Server hostname:  https://skyatp.argon.junipersecurity.net
  Server port:      443
  Control Plane:
    Connection Time: 2015-11-23 12:09:55 PST
    Connection Status: Connected
  Service Plane:
    fpc0
      Connection Active Number: 0
      Connection Failures: 0

```

Once configured, the SRX Series device communicates to the cloud through multiple persistent connections established over a secure channel (TLS 1.2) and the SRX device is authenticated using SSL client certificates.

As stated earlier, the script performs basic Juniper Sky ATP configuration on the SRX Series device. These include:

**NOTE:** You should not copy the following examples and run them on your SRX Series device. The list here is simply to show you what is being configured by the ops script. If you run into any issues, such as certificates, rerun the ops script again.

- Creating a default profile.
- Establishing a secured connection to the cloud server. The following is an example. Your exact URL is determined by your geographical region. Refer to this table.

Location	Customer Portal URL
United States	Customer Portal: <a href="https://amer.sky.junipersecurity.net">https://amer.sky.junipersecurity.net</a>
European Union	Customer Portal: <a href="https://euapac.sky.junipersecurity.net">https://euapac.sky.junipersecurity.net</a>
APAC	Customer Portal: <a href="https://apac.sky.junipersecurity.net">https://apac.sky.junipersecurity.net</a>
Canada	Customer Portal: <a href="https://canada.sky.junipersecurity.net">https://canada.sky.junipersecurity.net</a>

```

set services advanced-anti-malware connection url
  https://amer.sky.junipersecurity.net (this URL is only an example and will not
  work for all locations).
set services advanced-anti-malware connection authentication tls-profile aamw-ssl

```

- Configuring the SSL proxy.

```
set services ssl initiation profile aamw-ssl trusted-ca aamw-secintel-ca
set services ssl initiation profile aamw-ssl client-certificate aamw-srx-cert
set services security-intelligence authentication tls-profile aamw-ssl
set services advanced-anti-malware connection authentication tls-profile aamw-ssl
set services ssl initiation profile aamw-ssl trusted-ca aamw-cloud-ca
```

- Configuring the cloud feeds (whitelists, blacklists and so forth.)

```
set services security-intelligence url https://cloudfeeds.sky.junipersecurity.net/
api/manifest.xml
set services security-intelligence authentication tls-profile aamw-ssl
```

Juniper Sky ATP uses SSL forward proxy as the client and server authentication. Instead of importing the signing certificate and its issuer's certificates into the trusted-ca list of client browsers, SSL forward proxy now generates a certificate chain and sends this certificate chain to clients. Certificate chaining helps to eliminate the need to distribute the signing certificates of SSL forward proxy to the clients because clients can now implicitly trust the SSL forward proxy certificate.

The following CLI commands load the local certificate into the PKID cache and load the certificate-chain into the CA certificate cache in PKID, respectively.

```
user@root> request security pki local-certificate load filename ssl_proxy_ca.crt key sslserver.key
certificate-id ssl-inspect-ca
```

```
user@root> request security pki ca-certificate ca-profile-group load ca-group-name ca-group-name
filename certificate-chain
```

where:

**ssl\_proxy\_ca.crt (Signing certificate)**—Is the SSL forward proxy certificate signed by the administrator or by the intermediate CA.

**sslserver.key**—Is the key pair.

**ssl-inspect-ca**—Is the certificate ID that SSL forward proxy uses in configuring the root-ca in the SSL forward proxy profile.

**certificate-chain**—Is the file containing the chain of certificates.

The following is an example of SSL forward proxy certificate chaining used by the op script.

```
request security pki local-certificate enroll certificate-id aamw-srx-cert ca-profile aamw-ca  
challenge-password *** subject CN=4rrgffbtew4puztj:model:sn email email-address
```

```
request security pki ca-certificate enroll ca-profile aamw-ca
```

Note that you cannot enroll the SRX Series device to Juniper Sky ATP if the SRX device is in FIPS mode due to a PKI limitation.

To check your certificates, see [“Troubleshooting Juniper Sky Advanced Threat Prevention: Checking Certificates” on page 224](#). We recommend that you re-run the op script if you are having certificate issues.

# 2

PART

## The Web Portal and Enrolling SRX Series Devices

---

[The Juniper Sky ATP Web Portal](#) | 31

[Enroll SRX Series Devices](#) | 43

---

# The Juniper Sky ATP Web Portal

## IN THIS CHAPTER

- Juniper Sky Advanced Threat Prevention Configuration Overview | 31
- Juniper Sky Advanced Threat Prevention Web UI Overview | 34
- Dashboard Overview | 37
- Reset Password | 38
- Recover Realm Name | 40

## Juniper Sky Advanced Threat Prevention Configuration Overview

Table 5 on page 31 lists the basic steps to configure Juniper Sky ATP.

**NOTE:** These steps assume that you already have your SRX Series device(s) installed, configured, and operational at your site.

Table 5: Configuring Juniper Sky ATP

Task	Description	For information, see
(optional) Update the administrator profile	Update your administrator profile to add more users with administrator privileges to your security realm and to set the thresholds for receiving alert emails. A default administrator profile is created when you register an account.  This step is done in the Web UI.	<i>Sky Advanced Threat Prevention Administrator Profile Overview</i>

Table 5: Configuring Juniper Sky ATP (continued)

Task	Description	For information, see
Enroll your SRX Series devices	<p>Select the SRX Series devices to communicate with Juniper Sky ATP. Only those listed in the management interface can send files to the cloud for inspection and receive results.</p> <p>This step is done in the Web UI and on your SRX Series device.</p>	<a href="#">“Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention” on page 43</a>
Set global configurations	<p>Select <b>Configure &gt; Global Configuration</b> to set the default threshold and optionally, e-mail accounts when certain thresholds are reached. For example, you can send e-mails to an IT department when thresholds of 5 are met and send e-mails to an escalation department when thresholds of 9 are met.</p>	Web UI tooltips and online help
(optional) Create whitelists and blacklists	<p>Create whitelists and blacklists to list network nodes that you trust and don’t trust. Whitelisted websites are trusted websites where files downloaded from do not need to be inspected. Blacklisted websites are locations from which downloads should be blocked. Files downloaded from websites that are not in the whitelist or blacklist are sent to the cloud for inspection.</p> <p>This step is done in the Web UI.</p>	<a href="#">“Whitelist and Blacklist Overview” on page 57</a>
(optional) Create the Juniper Sky ATP profile	<p>Juniper Sky ATP profiles define which file types are to be sent to the cloud for inspection. For example, you may want to inspect executable files but not documents. If you don’t create a profile, the default one is used.</p> <p>This step is done in the Web UI.</p>	<a href="#">Juniper Sky Advanced Threat Prevention Profile Overview</a>
(optional) Identify compromised hosts	<p>Compromised hosts are systems where there is a high confidence that attackers have gained unauthorized access. Once identified, Juniper Sky ATP recommends an action and you can create security policies to take enforcement actions on the inbound and outbound traffic on these infected hosts.</p> <p>This step is done on the SRX Series device.</p>	<a href="#">“Compromised Hosts: More Information” on page 142</a>

Table 5: Configuring Juniper Sky ATP (continued)

Task	Description	For information, see
(optional) Block outbound requests to a C&C host	<p>The SRX Series device can intercept and perform an enforcement action when a host on your network tries to initiate contact with a possible C&amp;C server on the Internet.</p> <p>This step is done on the SRX Series device.</p> <p><b>NOTE:</b> Requires Juniper Sky ATP premium license.</p>	<p><a href="#">“Command and Control Servers: More Information”</a> on page 158</p>
Configure the Advanced Anti-Malware Policy on the SRX Series Device	<p>Advanced anti-malware security policies reside on the SRX Series device and determine which conditions to send files to the cloud and what to do when a file when a file receives a verdict number above the configured threshold.</p> <p>This step is done on the SRX Series device.</p>	<p><a href="#">“Juniper Sky Advanced Threat Prevention Policy Overview”</a> on page 193</p>
Configure the Security Intelligence Policy on the SRX Series Device	<p>Create the security intelligence policies on the SRX Series device to act on infected hosts and attempts to connect with a C&amp;C server.</p> <p>This step is done on the SRX Series device.</p>	<p><a href="#">“Configuring the SRX Series Devices to Block Infected Hosts”</a> on page 149</p> <p><a href="#">“Configuring the SRX Series Device to Block Outbound Requests to a C&amp;C Host”</a> on page 161</p>
Enable the firewall policy	<p>Create your SRX Series firewall policy to filter and log traffic in the network using the <b>set security policies from-zone to-zone</b> CLI commands.</p> <p>This step is done on the SRX Series device.</p>	<p><a href="#">“Configuring the SRX Series Devices to Block Infected Hosts”</a> on page 149</p> <p><a href="#">“Configuring the SRX Series Device to Block Outbound Requests to a C&amp;C Host”</a> on page 161</p> <p><a href="#">“Example: Configuring a Juniper Sky Advanced Threat Prevention Policy Using the CLI”</a> on page 197</p>

You can optionally use APIs for C&C feeds, whitelist and blacklist operations, and file submission. See the [Threat Intelligence Open API Setup Guide](#) for more information.

**NOTE:**

The cloud sends data, such as your Juniper Sky ATP whitelists, blacklists and profiles, to the SRX Series device every few seconds. You do not need to manually push your data from the cloud to your SRX Series device. Only new and updated information is sent; the cloud does not continually send all data.

## Juniper Sky Advanced Threat Prevention Web UI Overview

The Juniper Sky ATP Web UI is a web-based service portal that lets you monitor malware download through your SRX Series devices. The Web UI is hosted by Juniper Networks in the cloud. There is no separate download for you to install on your local system.

**NOTE:** If you are a licensed Junos Space Security Director, you can use Security Director 16.1 and later screens to set up and use Juniper Sky ATP. For more information using Security Director with Juniper Sky ATP, see the [Policy Enforcer](#) administration guide and the Security Director online help. The remainder of this guide refers to using Juniper Sky ATP with the Web UI.

You can perform the following tasks with the Web UI:

- **Monitoring**—Display information about scanned files whether clean or malware, infected hosts including their current and past threats, and blocked access to known C&C sites.
- **Configuring**—Create and view whitelists and blacklists that list safe or harmful network nodes, and profiles that define what file types to submit to Juniper Sky ATP for investigation.
- **Reporting**—Use the dashboard to view and drill into various reports, such as most infected file types, top malwares identified, and infected hosts.

The Web UI has infotips that provide information about a specific screen, field or object. To view the infotip, hover over the question mark (?) without clicking it. See.

### Accessing the Web UI

To access the Juniper Sky ATP Web UI:

1. Open a Web browser that has Hypertext Transfer Protocol (HTTP) or HTTP over Secure Sockets Layer (HTTPS) enabled.



For information on supported browsers and their version numbers, see the *Juniper Sky Advanced Threat Prevention Supported Platforms Guide*.

2. Type in the URL for the customer portal and press Enter.

The customer portal hostname varies by location. Please refer to the following table:

Location	Customer Portal URL
United States	Customer Portal: <a href="https://amer.sky.junipersecurity.net">https://amer.sky.junipersecurity.net</a>
European Union	Customer Portal: <a href="https://eu.sky.junipersecurity.net">https://eu.sky.junipersecurity.net</a>
APAC	Customer Portal: <a href="https://apac.sky.junipersecurity.net">https://apac.sky.junipersecurity.net</a>
Canada	Customer Portal: <a href="https://canada.sky.junipersecurity.net/">https://canada.sky.junipersecurity.net/</a>

The Web UI login page appears. See [Figure 13 on page 36](#).

Figure 13: Juniper Sky ATP Web UI Login Page

Sky ATP  
Version 3.0 | Login

E-mail Address

Password

Realm

Remember me

Log In

Create a Security Realm  
Forgot Password  
Forgot Realm

Supported JUNOS Software  
and Documentation

3. On the login page, type your username (your account e-mail address), password, and realm name and click **Log In**.

The Web UI Dashboard page appears.

**NOTE:** Users can login to Juniper Sky ATP using different realms. You can manage realms using the **Configure > Global Configuration > Realm Management** page. See [“Realm Overview” on page 122](#). You must be a system administrator to see the Realm Management page. See [“Creating and Editing User Profiles” on page 211](#) for information on role-based access control.

To terminate your session at any time, click the icon in the upper-right corner and click **Logout**.

## Dashboard Overview

The Juniper Sky Advanced Threat Prevention Web UI is a Web-based service portal that lets you monitor malware downloaded through your SRX Series devices.

The Web UI for Juniper Sky ATP includes a dashboard that provides a summary of all gathered information on compromised content and hosts. Drag and drop widgets to add them to your dashboard. Mouse over a widget to refresh, remove, or edit the contents.

In addition, you can use the dashboard to:

- Navigate to the File Scanning page from the Top Scanned Files and Top Infected Files widgets by clicking the More Details link.
- Navigate to the Hosts page from the Top Compromised Hosts widget by clicking the **More Details** link.
- Navigate to the Command and Control Servers page from the C&C Server Malware Source Location widget.

**NOTE:** C&C and GeolIP filtering feeds are only available with the Basic-Threat Feed or Premium license. For information on other licensed features, see *Juniper Sky Advanced Threat Prevention License Types*.

Available dashboard widgets are as follows:

**Table 6: Juniper Sky ATP Dashboard Widgets**

Widget	Definition
Top Malware Identified	A list of the top malware found based on the number of times the malware is detected over a period of time. Use the arrow to filter by different time frames.
Top Compromised Hosts	A list of the top compromised hosts based on their associated threat level and blocked status.
Top Infected File Types	A graph of the top infected file types by file extension. Examples: exe, pdf, ini, zip. Use the arrows to filter by threat level and time frame.
Top Infected File Categories	A graph of the top infected file categories. Examples: executables, archived files, libraries. Use the arrows to filter by threat level and time frame.
Top Scanned File Types	A graph of the top file types scanned for malware. Examples: exe, pdf, ini, zip. Use the arrows to filter by different time frames.

Table 6: Juniper Sky ATP Dashboard Widgets (continued)

Widget	Definition
Top Scanned File Categories	A graph of the top file categories scanned for malware. Examples: executables, archived files, libraries. Use the arrows to filter by different time frames.
C&C Server and Malware Source	A color-coded map displaying the location of Command and Control servers or other malware sources. Click a location on the map to view the number of detected sources.

## RELATED DOCUMENTATION

[Reset Password](#) | 38

[Juniper Sky Advanced Threat Prevention](#) | 2

[How is Malware Analyzed and Detected?](#) | 9

[Hosts Overview](#) | 137

[HTTP File Download Overview](#) | 164

[Command and Control Servers Overview](#) | 153

## Reset Password

If you forget your password to login to the Juniper Sky ATP dashboard, you can reset it using a link sent by email when you click **Forgot Password** from the Juniper Sky ATP login screen. The following section provides details for resetting your password securely over email.

- To reset your password you must enter the realm name and a valid email address.
- Once you receive your password reset email, the link expires immediately upon use or within one hour. If you want to reset your password again, you must step through the process to receive a new link.
- Use this process if you have forgotten your password. If you are logged into the dashboard and want to change your password, you can do that from the **Administration > My Profile** page. See [“Modifying My Profile” on page 210](#) for those instructions.

To reset your Juniper Sky ATP dashboard password, do the following:

1. Click the **Forgot Password** link on the Juniper Sky ATP dashboard login page.
2. In the screen that appears, enter the **Email address** associated with your account.

3. Enter the **Realm** name.
4. Click **Continue**. An email with a link for resetting your password is sent. Note that the link expires within one hour of receiving it.
5. Click the link in the email to go to the Reset Password page.
6. Enter a new password and then enter it again to confirm it. The password must contain an uppercase and a lowercase letter, a number, and a special character.
7. Click **Continue**. The password is now reset. You should receive an email confirming the reset action. You can now login with the new password.

#### RELATED DOCUMENTATION

[Modifying My Profile | 210](#)

---

[Creating and Editing User Profiles | 211](#)

---

[Dashboard Overview | 37](#)

## Recover Realm Name

If you forget your realm name to login to the Juniper Sky ATP portal, you can recover the realm name using the following methods:

- See the confirmation e-mail that is sent to you when you create a new realm. The e-mail now contains the realm name. Here's a sample:

```
Welcome to Juniper SkyATP!

You have successfully created your SkyATP Security Realm. Below is your information:
You email ID: user@juniper.net

Realm Name: " realm123"

You may save the Realm name for future use for login purpose as SkyATP login expects
Realm name as an input.

You can login now using link: https://xxxxxxxx

Please do not reply to this automated message and contact JTAC if you have any
questions.

Thank you,
Your friendly Juniper Sky ATP robot.
```

- Click **Forgot Realm** link from the Juniper Sky ATP login page.

The following section provides details to recover the realm name using the Juniper Sky ATP web portal.

**NOTE:** To recover the realm name you must enter a valid e-mail address.

To recover the realm name from the Sky ATP web portal:

1. Open a Web browser, type in the URL for the Sky ATP web portal, and press **Enter**.

The login page appears as shown in [Figure 14 on page 41](#).

Figure 14: Juniper Sky ATP Web UI Login Page

Sky ATP  
Version 3.0 | Login

E-mail Address

Password

Realm

Remember me

Log In

[Create a Security Realm](#)  
[Forgot Password](#)  
[Forgot Realm](#)

[Supported JUNOS Software and Documentation](#)

2. Click the **Forgot Realm** link.

A pop-up appears asking you to confirm navigation to customer support center to provide Juniper SSO credentials.

3. Click **Continue**.

The customer support center login page appears.

4. Enter the e-mail address that you provided while creating the realm and click **Next**.

A pop-up message is displayed with the status of realm recovery.

- If the e-mail address has realms associated with it, an e-mail is sent to your registered e-mail address with the list of associated realms. Here's a sample:

```
An email message has been sent to user@juniper.net with the names of all Sky
ATP Realms associated with this email address.
```

Here's a sample e-mail for realm recovery:

```
Welcome to Juniper SkyATP !

Based on your request please find below Realms created by you with Juniper
SkyATP till date.

Your email ID : <Juniper-Networks-Account>

Realm names: REALM-1, REALM-2, RELAM-3...REALM-N

You may save the Realm name for future use for login purpose as SkyATP login
expects Realm name as an input.

You can login now using link: <realm-recovery link>

Please do not reply to this automated message and contact JTAC if you have any
questions.

Thank you,
Your friendly Juniper Sky ATP robot
```

- If no realms are associated with the e-mail address, then you will see the following message:

```
There are no realms created by login user@juniper.net.
```

5. Click **OK** to login to the Sky ATP portal with the realm name.

## RELATED DOCUMENTATION

[Reset Password | 38](#)

[Dashboard Overview | 37](#)



# Enroll SRX Series Devices

## IN THIS CHAPTER

- Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention | 43
- Enrolling an SRX Series Device without the Juniper Sky ATP Web Portal | 47
- Removing an SRX Series Device From Juniper Sky Advanced Threat Prevention | 49
- Searching for SRX Series Devices Within Juniper Sky Advanced Threat Prevention | 50
- Juniper Sky Advanced Threat Prevention RMA Process | 53
- Device Information | 53
- Cloud Feeds for Juniper Sky Advanced Threat Prevention: More Information | 54

## Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention

Only devices enrolled with Juniper Sky ATP can send files for malware inspection.

Before enrolling a device, check whether the device is already enrolled. To do this, use the Devices screen or the Device Lookup option in the Web UI (see [“Searching for SRX Series Devices Within Juniper Sky Advanced Threat Prevention” on page 50](#)). If the device is already enrolled, disenroll it first before enrolling it again.

**NOTE:** If a device is already enrolled in a realm and you enroll it in a new realm, none of the device data or configuration information is propagated to the new realm. This includes history, infected hosts feeds, logging, API tokens, and administrator accounts.

**NOTE:** In the Enrolled Devices page, you can view the realm with which the device is associated. From the Realm Management page, you can change that realm association or attach new realms. See [“Realm Management” on page 124](#) for configuration details.

As of Junos Release 19.3R1, there is another way to enroll the SRX Series device without having to interact with the Sky ATP Web Portal. You run the “enroll” command from the SRX and it performs all the necessary enrollment steps. See [“Enrolling an SRX Series Device without the Juniper Sky ATP Web Portal” on page 47](#)

Juniper Sky ATP uses a Junos OS operation (op) script to help you configure your SRX Series device to connect to the Juniper Sky Advanced Threat Prevention cloud service. This script performs the following tasks:

- Downloads and installs certificate authority (CAs) licenses onto your SRX Series device.
- Creates local certificates and enrolls them with the cloud server.
- Performs basic Juniper Sky ATP configuration on the SRX Series device.
- Establishes a secure connection to the cloud server.

**NOTE:** Juniper Sky Advanced Threat Prevention requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) can connect to the Internet. Juniper Sky Advanced Threat Prevention requires the following ports to be open on the SRX Series device: 80, 8080, and 443.



**WARNING:** If you are configuring explicit web proxy support for SRX Series services/Juniper Sky ATP connections, you must enroll SRX Series devices to Juniper Sky ATP using a slightly different process, see [“Explicit Web Proxy Support” on page 204](#).

To enroll a device in Juniper Sky ATP using the Web Portal, do the following:

1. Click the **Enroll** button on the Devices page.
2. Copy the command to your clipboard and click **OK**.
3. Paste the command into the Junos OS CLI of the SRX Series device you want to enroll with Juniper Sky ATP and press **Enter**. (Note that this command must be run in operational mode.)

**NOTE:** If the script fails, disenroll the device (see instructions for disenrolling devices) and then re-enroll it.

**NOTE:** (Optional) Use the **show services advanced-anti-malware status** CLI command to verify that a connection is made to the cloud server from the SRX Series device.

Once configured, the SRX Series device communicates to the cloud through multiple persistent connections established over a secure channel (TLS 1.2) and the SRX Series device is authenticated using SSL client certificates.

In the Juniper Sky ATP Web UI Enrolled Devices page, basic connection information for all enrolled devices is provided, including serial number, model number, tier level (free or not) enrollment status in Juniper Sky ATP, last telemetry activity, and last activity seen. Click the serial number for more details. In addition to Enroll, the following buttons are available:

**Table 7: Button Actions**

Actions	Definition
Enroll	Use the Enroll button to obtain a enroll command to run on eligible SRX Series devices. This command enrolls them in Juniper Sky ATP and is valid for 7 days. Once enrolled, SRX Series device appears in the Devices and Connections list.
Disenroll	Use the Disenroll button to obtain a disenroll command to run on SRX Series devices currently enrolled in Juniper Sky ATP. This command removes those devices from Juniper Sky ATP enrollment and is valid for 7 days.

**NOTE:** Running the Enroll or Disenroll command will commit any uncommitted configuration changes on the SRX Series device.

**NOTE:** Generating a new Enroll or Disenroll command invalidates any previously generated commands.

Device Lookup	Use the Device Lookup button to search for the device serial number(s) in the licensing database to determine the tier (premium, feed only, free) of the device. For this search, the device does not have to be currently enrolled in Juniper Sky ATP.
Remove	Removing an SRX Series device is different than disenrolling it. Use the Remove option only when the associated SRX Series device is not responding (for example, hardware failure). Removing it, disassociates it from the cloud without running the Junos OS operation (op) script on the device (see Enrolling and Disenrolling Devices). You can later enroll it using the Enroll option when the device is again available.

For HA configurations, you only need to enroll the cluster master. The cloud will detect that this is a cluster and will automatically enroll both the master and slave as a pair. Both devices, however, must be licensed accordingly. For example, if you want premium features, both devices must be entitled with the premium license.

**NOTE:** Juniper Sky ATP supports only the active-passive cluster configuration. The passive (non-active) node does not establish a connection to the cloud until it becomes the active node. Active-active cluster configuration is not supported.

**NOTE:** The License Expiration column contains the status of your current license, including expiration information. There is a 60 day grace period after the license expires before the SRX Series device is disenrolled from Juniper Sky ATP. On the SRX Series device, you can run the > **show system license** command to view license details.

## RELATED DOCUMENTATION

[Juniper Sky Advanced Threat Prevention RMA Process | 53](#)

[Removing an SRX Series Device From Juniper Sky Advanced Threat Prevention | 49](#)

[Searching for SRX Series Devices Within Juniper Sky Advanced Threat Prevention | 50](#)

[Device Information | 53](#)

## Enrolling an SRX Series Device without the Juniper Sky ATP Web Portal

Starting in Junos OS Release 19.3R1, you can use the **request services advanced-anti-malware enroll** command on the SRX Series to enroll a device to the Juniper Sky ATP Web Portal. With this command, you do not have to perform any enrollment tasks on the Web Portal itself. All enrollment is done from the CLI on the SRX.

Enrollment establishes a secure connection between the Juniper Sky ATP cloud server and the SRX Series device. It also performs basic configuration tasks such as:

- Downloads and installs certificate authorities (CAs) onto your SRX Series device
- Creates local certificates and enrolls them with the cloud server
- Establishes a secure connection to the cloud server

**NOTE:** Juniper Sky Advanced Threat Prevention requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) can connect to the Internet. You do not need to open any ports on the SRX Series device to communicate with the cloud server. However, if you have a device in the middle, such as a firewall, then that device must have ports 80, 8080, and 443 open.

Also note, the SRX Series device must be configured with DNS servers in order to resolve the cloud URL.

Using the device enrollment command on the SRX Series device, **request services advanced-anti-malware enroll**, you can enroll the device to an existing realm or create a new realm and then enroll to it.

Here is an example configuration that creates a new realm and then enrolls to that realm.

```
root@host> request services advanced-anti-malware enroll
```

1. Enroll the SRX Series device to Juniper Sky ATP (CLI only):

```
user@host> request services advanced-anti-malware enroll
```

Please select geographical region from the list:

1. North America
2. European Region
3. Canada
4. Asia Pacific

Your choice: 1

2. Select an existing realm or create a new realm:

**Enroll SRX to:**

1. A new SkyATP security realm (you will be required to create it first)
2. An existing SkyATP security realm

If you select option 1 to create a new realm, the steps are as follows:

- You are going to create a new Sky ATP realm, please provide the required information:
- Please enter a realm name (This should be a name that is meaningful to your organization. A realm name can only contain alphanumeric characters and the dash symbol. Once a realm is created, it cannot be changed):

Real name: example-company-a

- Please enter your company name:

Company name: Example Company A

- Please enter your e-mail address. This will be your username for your Sky ATP account:

Email: me@example-company-a.com

- Please setup a password for your new Sky ATP account (It must be at least 8 characters long and include both uppercase and lowercase letters, at least one number, at least one special character):

Password: \*\*\*\*\*

Verify: \*\*\*\*\*

- Please review the information you have provided:

Region: North America

New Realm: example-company-a

Company name: Example Company A

Email: me@example-company-a.com

- Create a new realm with the above information? [yes,no]

yes

**Device enrolled successfully!**

If you select option 2 to use an existing realm, the steps are as follows:

**NOTE:** You must enter a valid username and password for the existing realm as part of the enrollment procedure.

- Enter the name of the existing realm:

Please enter a realm name.

Realm name: example-company-b

- Please enter your company name:

Company name: Example Company B

- Enter your email address/username for the realm. This is the email address that was previously created when setting up the realm.

Please enter your e-mail address. This will be your username for your Sky ATP account:

- Enter the password for the realm. This is the password that was previously created when setting up the realm.

Password:\*\*\*\*\*

- Enroll device to the realm above? [yes,no] yes

Device enrolled successfully!

You can use the **show services advanced-anti-malware status** CLI command on your SRX Series device to verify that a connection has been made to the cloud server from the SRX Series device.

Once enrolled, the SRX Series device communicates to the cloud through multiple, persistent connections established over a secure channel (TLS 1.2) and the SRX Series device is authenticated using SSL client certificates.

## RELATED DOCUMENTATION

| [Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention](#) | 43

## Removing an SRX Series Device From Juniper Sky Advanced Threat Prevention

If you no longer want an SRX Series device to send files to the cloud for inspection, use the disenroll option to disassociate it from Juniper Sky Advanced Threat Prevention. The disenroll process generates an ops script to be run on SRX Series devices and resets any properties set by the enroll process.

To disenroll an SRX Series device:

1. Select the check box associated with the device you want to disassociate and click **Disenroll**.
2. Copy the highlighted command to your clipboard and click **OK**.

3. Paste this command into the Junos OS CLI of the device you want to disenroll and press **Enter**.

You can re-enroll this device at a later time using the Enroll option.

#### RELATED DOCUMENTATION

[Searching for SRX Series Devices Within Juniper Sky Advanced Threat Prevention | 50](#)

[Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention | 43](#)

[Device Information | 53](#)

## Searching for SRX Series Devices Within Juniper Sky Advanced Threat Prevention

You can search for any SRX Series device enrolled within your security realm of Juniper Sky Advanced Threat Prevention using the Device Lookup option. This option also a way for you to view the type of license the device is using: basic, premium, or free. .

**NOTE:** With this release, you can only search for device using serial numbers.

To search for devices enrolled with Juniper Sky Advanced Threat Prevention:

1. From the Web UI, select **Devices**.
2. Click **Device Lookup**.

The Device Lookup window appears. See [Figure 15 on page 51](#).



Figure 15: Searching for a Device in the Web UI

The screenshot shows a web interface titled "Untitled" with a help icon. A progress indicator at the top shows two steps: "1 Enter Serial Numbers" (highlighted in blue) and "2 Search results" (greyed out). Below the progress indicator, the label "Untitled" is followed by the text "Serial Number(s) \*" and a large empty text input field. At the bottom of the form, there are two buttons: "Cancel" on the left and "Next" on the right, which is highlighted in blue.

3. Enter the serial number of the device you want to search for and click **Next**. You can enter multiple serial numbers, separating each entry with a comma. For more information, see the infotips.

**NOTE:** The Web UI does not check for valid serial numbers. If you enter an invalid serial number, the results will come back empty. If you enter multiple serial numbers and one is an invalid number, the results will come back empty.

The search results window appears. See [Figure 16 on page 52](#).

Figure 16: Example Device Search Results

Untitled ?

1 — 2

Enter Serial Numbers      Search results

**Untitled**

Serial Number	Model Number	Tier
UKLG0YN0OAOI	SRX100	free
UVPT50UEC4D	SRX100	free
EHR7QC24NLNX	SRX5800	free
ERTUFB86XB0W	SRX5800	free
DFLA939OP6RT	SRX5600	premium

Cancel      Back      OK

- (Optional) Click a serial number to view details about that device.

#### RELATED DOCUMENTATION

[Device Information | 53](#)

[Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention | 43](#)

[Removing an SRX Series Device From Juniper Sky Advanced Threat Prevention | 49](#)

[Searching for SRX Series Devices Within Juniper Sky Advanced Threat Prevention | 50](#)

## Juniper Sky Advanced Threat Prevention RMA Process

On occasion, because of hardware failure, a device needs to be returned for repair or replacement. For these cases, contact Juniper Networks, Inc. to obtain a Return Material Authorization (RMA) number and follow the [RMA Procedure](#).

Once you transfer your license keys to the new device, it may take up to 24 hours for the new serial number to be registered with the Juniper Sky ATP cloud service.



**WARNING:** After any serial number change on the SRX Series device, a new RMA serial number needs to be re-enrolled with Juniper Sky ATP cloud. This means that you must enroll your replacement unit as a new device. See [“Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention” on page 43](#). Juniper Sky ATP does not have an “RMA state”, and does not see these as replacement devices from a configuration or registration point of view. Data is not automatically transferred to the replacement SRX Series device from the old device.

## Device Information

Use this page to view the following information on the selected SRX Series device.

**Table 8: Device Information Fields**

Field	Definition
Device Information	
Serial Number	SRX Series device serial number
Host	Host name of the device.
Model Number	SRX Series device model number
Tier	License type: Free, Feed only, Premium.
OS Version	SRX Series device JunOS version
Submission Status	Allowed or Paused. This indicates whether the device can submit files to Juniper Sky ATP or if it has reached its daily limit. (At this time, the limit is 10,000 files per day for premium accounts.)

Table 8: Device Information Fields (continued)

Field	Definition
Configuration Information	
Global Config	The Device and Cloud fields indicate the version numbers of each list, both on the device and in the cloud. You can compare them to see if they are in sync.
Profile Config	
Global Whitelist	
Global Blacklist	
Customer Whitelist	
Customer Blacklist	
Connection Type	
Telemetry	The time when the last telemetry submission was received.
Submission	The time when the last file submission was received.
C&C Event	The time when the last Command and Control event was received.

## RELATED DOCUMENTATION

[Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention | 43](#)

[Removing an SRX Series Device From Juniper Sky Advanced Threat Prevention | 49](#)

[Searching for SRX Series Devices Within Juniper Sky Advanced Threat Prevention | 50](#)

## Cloud Feeds for Juniper Sky Advanced Threat Prevention: More Information

The cloud feed URL is set up automatically for you when you run the op script to configure your SRX Series device. See “[Downloading and Running the Juniper Sky Advanced Threat Prevention Script](#)” on page 24. There are no further steps you need to do to configure the cloud feed URL.

If you want to check the cloud feed URL on your SRX Series device, run the **show services security-intelligence URL** CLI command. Your output should look similar to the following:

```
root@host# show services security-intelligence url
https://cloudfeeds.sky.junipersecurity.net/api/manifest.xml
```

If you do not see a URL listed, run the ops script again as it configures other settings in addition to the cloud feed URL.

### SRX Series Update Intervals for Cloud Feeds

The following table provides the update intervals for each feed type. Note that when the SRX Series device makes requests for new and updated feed content, if there is no new content, no updates are downloaded at that time.

**NOTE:** You can run the **request services security-intelligence download** command to manually download updates before the next interval, although this is not recommended.

**Table 9: Feed Update Intervals**

Category	Feeds	SRX Update Intervals (in seconds)
Command and Control	Juniper Feeds	1,800
	Integrated Feeds	1,800
	Customer Feeds	1,800
GeoIP	geoip_country	435,600
Whitelist	Customer Feeds	3,600
Blacklist	Customer Feeds	3,600
Infected Hosts	Infected Hosts	60
IPFilter	Customer Feeds	1,800
	Office 365	1,800

# 3

PART

## Configure

---

[Whitelists and Blacklists | 57](#)

[Email Scanning: Juniper Sky ATP | 65](#)

[Email Scanning: SRX Series Device | 74](#)

[File Inspection Profiles | 92](#)

[Adaptive Threat Profiling | 97](#)

[Third Party Threat Feeds | 110](#)

[Global Configurations | 116](#)

---

# Whitelists and Blacklists

## IN THIS CHAPTER

- [Whitelist and Blacklist Overview | 57](#)
- [Creating Whitelists and Blacklists | 59](#)

## Whitelist and Blacklist Overview

A whitelist contains known trusted IP addresses, Hashes, Email addresses, and URLs. Content downloaded from locations on the whitelist does not have to be inspected for malware. A blacklist contains known untrusted IP addresses and URLs. Access to locations on the blacklist is blocked, and therefore no content can be downloaded from those sites.

### Benefits of Whitelists and Blacklists

- Whitelists allows users to download files from sources that are known to be safe. Whitelists can be added to in order to decrease false positives.
- Blacklists prevent users from downloading files from sources that are known to be harmful or suspicious.

The Custom whitelists or custom blacklists allow you to add items manually. Both are configured on the Juniper Sky ATP cloud server. The priority order is as follows:

1. Custom whitelist
2. Custom blacklist

If a location is in multiple lists, the first match wins.

Whitelists and blacklists support the following types:

- URL
- IP address
- Hostname
- Hash file

**NOTE:**

- For IP and URL, The Web UI performs basic syntax checks to ensure your entries are valid.
- The cloud feed URL for whitelists and blacklists is set up automatically for you when you run the op script to configure your SRX Series device. See [“Downloading and Running the Juniper Sky Advanced Threat Prevention Script” on page 24.](#)
- A hash is a unique signature for a file generated by an algorithm. You can add custom whitelist and blacklist hashes for filtering, but they must be listed in a text file with each entry on a single line. You can only have one running file containing up to 15,000 file hashes. For upload details see [“Creating Whitelists and Blacklists” on page 59.](#) Note that Hash lists are slightly different than other list types in that they operate on the cloud side rather than the SRX Series device side. This means the web portal is able to display hits on hash items.

The SRX series device makes requests approximately every two hours for new and updated feed content. If there is nothing new, no new updates are downloaded.

Use the **show security dynamic-address instance advanced-anti-malware** CLI command to view the IP-based whitelists and blacklists on your SRX Series device. There is no CLI command to show the domain-based or URL-based whitelists and blacklists at this time.

**Example show security dynamic-address instance advanced-anti-malware**

```
user@host>show security dynamic-address instance advanced-anti-malware
No.      IP-start      IP-end      Feed      Address
1        x.x.x.0      x.x.x.10   custom_whitelist ID-80000400
2        x.x.0.0      x.x.0.10   custom_blacklist ID-80000800

Instance advanced-anti-malware Total number of matching entries: 2
```

If you do not see your updates, wait a few minutes and try the command again. You might be outside the Juniper Sky ATP polling period.

Once your whitelists or blacklists are created, create an advanced anti-malware policy to log (or don't log) when attempting to download a file from a site listed in the blacklist or white list files. For example, the following creates a policy named **aawmpolicy1** and creates log entries.

```
set services advanced-anti-malware policy aawmpolicy1 blacklist-notification log
set services advanced-anti-malware policy aawmpolicy1 whitelist-notification log
```

**RELATED DOCUMENTATION**



## Creating Whitelists and Blacklists

Access these pages from **Configure > Whitelists** or **Blacklists**.

Use the whitelist and blacklist pages to configure custom trusted and untrusted lists. You can also upload hash files.

Content downloaded from locations on the whitelist is trusted and does not have to be inspected for malware. Hosts cannot download content from locations on the blacklist, because those locations are untrusted.

- Read the “[Whitelist and Blacklist Overview](#)” on page 57 topic.
- Decide on the type of item you intend to define: URL, IP, Hash, Domain
- Review current list entries to ensure the item you are adding does not already exist.
- If you are uploading hash files, the files must be in a text file with each hash on its own single line.

To create Juniper Sky ATP whitelists and blacklists:

1. Select **Configuration > Whitelist** or **Blacklist**.
2. For either Whitelist or Blacklist, select one of the following tabs: **IP and URL**, **Hash File**, **Email Sender**, **C&C Server**, or **Encrypted Traffic** and enter the required information. See the tables below.

**NOTE:** **Encrypted Traffic** option is available only under **Whitelist** menu.

3. Click **OK**.

Refer to the following tables for the data required by each tab.

### IP and URL

When you create a new IP or URL list item, you must choose the Type of list: **IP** or **URL**. You can do this by selecting the type in the navigation pane or by choosing it from a pulldown list in the Create window. Depending on the type, you must enter the required information. See the following table.

Table 10: IP and URL Configuration

Setting	Guideline
IP	<p>Enter the IPv4 or IPv6 IP address. For example: 1.2.3.4 or 0:0:0:0:FFFF:0102:0304. CIDR notation and IP address ranges are also accepted.</p> <p>Any of the following IPv4 formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6.</p> <p>Any of the following IPv6 formats are valid: 1111::1, 1111::1-1111::9, or 1111:1::0/64.</p> <p><b>NOTE:</b> Address ranges: No more than a block of /16 IPv4 addresses and /48 IPv6 addresses are accepted. For example, 10.0.0.0-10.0.255.255 is valid, but 10.0.0.0-10.1.0.0 is not.</p> <p>Bitmasks: The maximum amount of IP addresses covered by bitmask in a subnet record for IPv4 is 16 and for IPv6 is 48. For example, 10.0.0.0/15 and 1234::/47 are not valid.</p>
URL	<p>Enter the URL using the following format: juniper.net. Wildcards and protocols are not valid entries. The system automatically adds a wildcard to the beginning and end of URLs. Therefore juniper.net also matches a.juniper.net, a.b.juniper.net, and a.juniper.net/abc. If you explicitly enter a.juniper.net, it matches b.a.juniper.net, but not c.juniper.net. You can enter a specific path. If you enter juniper.net/abc, it matches x.juniper.net/abc, but not x.juniper.net/123.</p>

**NOTE:** To edit an existing whitelist or blacklist IP or URL entry, select the check box next to the entry you want to edit and click the pencil icon.

## Hash File

When you upload a hash file, it must be in a text file with each hash on its own single line. You can only have one running hash file. To add to it or edit it, see the instructions in the following table.

Table 11: Hash File Upload and Edit

Field	Guideline
	<p>You can add custom whitelist and blacklist hashes for filtering, but they must be listed in a text file with each entry on a single line. You can only have one running hash file containing up to 15,000 file hashes. This is the “current” list, but you can add to it, edit it, and delete it at any time.</p>

Table 11: Hash File Upload and Edit (*continued*)

Field	Guideline
SHA-256 Hash Item	<p>To add to hash entries, you can upload several text files and they will automatically combine into one file. See all, merge, delete and replace options below.</p> <p><b>Download</b>—Click this button to download the text file if you want to view or edit it.</p> <p>You have the following options from the pulldown:</p> <ul style="list-style-type: none"> <li>• <b>Replace current list</b>—Use this option when you want to change the existing list, but do not want to delete it entirely. Download the existing file, edit it, and then upload it again.</li> <li>• <b>Merge with current list</b>—Use this option when you upload a new text file and want it to combine with the existing text file. The hashes in both files combine to form one text file containing all hashes.</li> <li>• <b>Delete from current list</b>—Use this option when you want to delete only a portion of the current list. In this case, you would create a text file containing only the hashes you want to remove from the current list. Upload the file using this option and only the hashes in the uploaded file are deleted from the current active list.</li> </ul> <p><b>Delete All</b> or <b>Delete Selected</b>—Sometimes it's more efficient to delete the current list rather than downloading it and editing it. Click this button to delete the current selected list or all lists that have been added and accumulated here.</p>
Source	This says either Whitelist or Blacklist.
Date Added	The month, date, year, and time when the hash file was last uploaded or edited.

### Email Sender

Add email addresses to be whitelisted or blacklisted if found in either the sender or recipient of an email communication. Add addresses one at a time using the + icon.

Table 12: Email Sender

Field	Guideline
Email address	Enter an email address in the format name@domain.com. Wildcards and partial matches are not supported, but if you want to include an entire domain, you could enter only the domain as follows: domain.com

Table 12: Email Sender (continued)

Field	Guideline
	<p>If an email matches the blacklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment. The email is blocked and a replacement email is sent. If an email matches the whitelist, that email is allowed through without any scanning. See <a href="#">“SMTP Quarantine Overview: Blocked Emails” on page 177</a>.</p> <p>It is worth noting that attackers can easily fake the “From” email address of an email, making blacklists a less effective way to stop malicious emails.</p>

### C&C Server

When you whitelist a C&C server, the IP or hostname is sent to the SRX Series devices to be excluded from any security intelligence blacklists or C&C feeds (both Juniper’s global threat feed and third party feeds). The server will also now be listed under the C&C whitelist management page.

You can enter C&C server data manually or upload a list of servers. That list must be a text file with each IP or Domain on its own single line. The text file must include all IPs or all Domains, each in their own file. You can upload multiple files, one at a time.

**NOTE:** You can also manage whitelist and blacklist entries using the Threat Intelligence API. When adding entries to the whitelist/blacklist data, these will be available in the Threat Intelligence API under the following feed names: “whitelist\_domain” or “whitelist\_ip”, and “blacklist\_domain” or “blacklist\_ip.” See the [Juniper Sky ATP Threat Intelligence Open API Setup Guide](#) for details on using the API to manage any custom feeds.

Table 13: C&amp;C Server

Field	Guideline
Type	Select IP to enter the IP address of a C&C server that you want to add to the whitelist. Select Domain to whitelist an entire domain on the C&C server list.
IP or Domain	For IP, enter an IPv4 or IPv6 address. An IP can be IP address, IP range or IP subnet. For domain, use the following syntax: juniper.net. Wildcards are not supported.
Description	Enter a description that indicates why an item has been added to the list.

Table 13: C&amp;C Server (continued)

Field	Guideline
-------	-----------

You can also whitelist C&C servers directly from the C&C Monitoring page details view. See [“Command and Control Server Details” on page 154](#).

**WARNING:** Adding a C&C server to the whitelist automatically triggers a remediation process to update any affected hosts (in that realm) that have contacted the whitelisted C&C server. All C&C events related to this whitelisted server will be removed from the affected hosts’ events, and a host threat level recalculation will occur.

If the host score changes during this recalculation, a new host event appears describing why it was rescored. (For example, “Host threat level updated after C&C server 1.2.3.4 was cleared.”) Additionally, the server will no longer appear in the list of C&C servers because it has been cleared.

## Encrypted Traffic

You can specify the IP address or domain names that you want to whitelist from encrypted traffic analysis. Use this tab to add, modify, or delete the whitelists for encrypted traffic analysis.

Table 14: Encrypted Traffic

Field	Guideline
Type	Select whether you want to specify the IP address or domain name for the whitelist.
IP or Domain	Enter the IP address or domain name for the whitelist.

**NOTE:** Juniper Sky ATP periodically polls for new and updated content and automatically downloads it to your SRX Series device. There is no need to manually push your whitelist or blacklist files.

Use the **show security dynamic-address instance advanced-anti-malware** command to view the custom whitelist and blacklist on SRX Series devices.

```
user@host>show security dynamic-address instance advanced-anti-malware
No.      IP-start      IP-end      Feed      Address
1        x.x.x.0      x.x.x.10   custom_whitelist ID-80000400
2        x.x.0.0      x.x.0.10   custom_blacklist ID-80000800

Instance advanced-anti-malware Total number of matching entries: 2
```

## RELATED DOCUMENTATION

[Whitelist and Blacklist Overview | 57](#)

[Enabling Third Party Threat Feeds | 110](#)

---

# Email Scanning: Juniper Sky ATP

## IN THIS CHAPTER

- Email Management Overview | 65
- Email Management: Configure SMTP | 67
- Email Management: Configure IMAP | 70

## Email Management Overview

With Email Management, enrolled SRX devices transparently submit potentially malicious email attachments to the cloud for inspection. Once an attachment is evaluated, Juniper Sky ATP assigns the file a threat score between 0-10 with 10 being the most malicious.

**NOTE:** If an email contains no attachments, it is allowed to pass without any analysis.

### Benefits of Email Management

- Allows attachments to be checked against whitelists and blacklists.
- Prevents users from opening potential malware received as an email attachment.

Configure Juniper Sky ATP to take one of the following actions when an email attachment is determined to be malicious:

### For SMTP

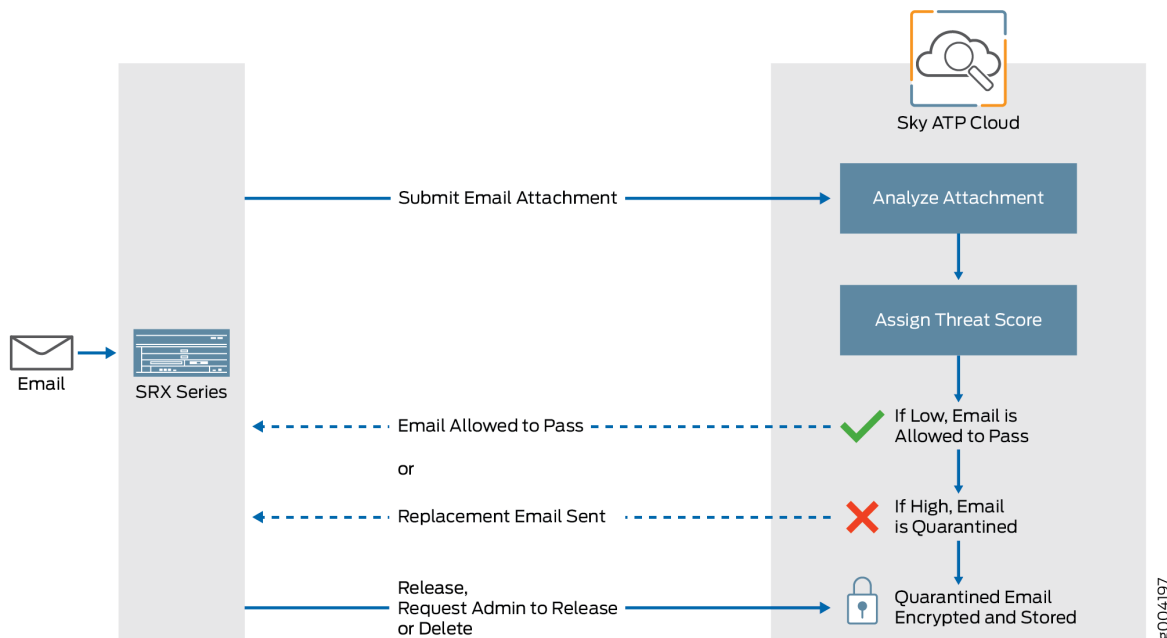
- Quarantine Malicious Messages—If you select to quarantine emails with attachments found to be malicious, those emails are stored in the cloud in an encrypted form and a replacement email is sent to the intended recipient. That replacement email informs the recipient of the quarantined message and provides a link to the Juniper Sky ATP quarantine portal where the email can be previewed. The recipient can then choose to release the email by clicking a Release button (or request that the administrator release it) or Delete the email.
- Deliver malicious messages with warning headers added—When you select this option, headers are added to emails that most mail servers recognize and filter into Spam or Junk folders.

- Permit—You can select to permit the email and the recipient receives it intact.

#### For IMAP

- Block Malicious Messages—Block emails with attachments that are found to be malicious.
- Permit—You can select to permit the email and the recipient receives it intact.

Figure 17: Email Management Overview



#### Quarantine Release

If the recipient selects to release a quarantined email, it is allowed to pass through the SRX series with a header message that prevents it from being quarantined again, but the attachments are placed in a password-protected ZIP file. The password required to open the ZIP file is also included as a separate attachment. The administrator is notified when the recipient takes an action on the email (either to release or delete it).

If you configure Juniper Sky ATP to have the recipient send a request to the administrator to release the email, the recipient previews the email in the Juniper Sky ATP quarantine portal and can select to Delete the email or Request to Release. The recipient receives a message when the administrator takes action (either to release or delete the email.)

#### Blacklist and Whitelist

Emails are checked against administrator-configured blacklists and whitelists using information such as Envelope From (MAIL FROM), Envelope To (RCPT TO), Body Sender, Body Receiver. If an email matches



the whitelist, that email is allowed through without any scanning. If an email matches the blacklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment.

## RELATED DOCUMENTATION

[Email Management: Configure SMTP | 67](#)

[Creating Whitelists and Blacklists | 59](#)

[SMTP Quarantine Overview: Blocked Emails | 177](#)

## Email Management: Configure SMTP

Access this page from **Configure > Email Management > SMTP**.

- Read the “[Email Management Overview](#)” on page 65 topic.
- Decide how malicious emails are handled: quarantined, delivered with headers, or permitted.

1. Select **Configure > Email Management > SMTP**.
2. Based on your selections, configuration options will vary. See the tables below.

**Table 15: Configure Quarantine Malicious Messages**

Setting	Guideline
Action to take	Quarantine malicious messages—When you select to quarantine malicious email messages, in place of the original email, intended recipients receive a custom email you configure with information on the quarantining. Both the original email and the attachment are stored in the cloud in an encrypted format.

Table 15: Configure Quarantine Malicious Messages (*continued*)

Setting	Guideline
Release option	<ul style="list-style-type: none"> <li>Recipients can release email—This option provides recipients with a link to the Juniper Sky ATP quarantine portal where they can preview the email. From the portal, recipients can select to <b>Release</b> the email or <b>Delete</b> it. Either action causes a message to be sent to the administrator.  <b>NOTE:</b> If a quarantined email has multiple recipients, any individual recipient can release the email from the portal and all recipients will receive it. Similarly, if one recipient deletes the email from the portal, it is deleted for all recipients.</li> <li>Recipients can request administrator to release email—This option also provides recipients with a link to the Juniper Sky ATP quarantine portal where they can preview the email. From the portal, recipients can select to <b>Request to Release</b> the email or <b>Delete</b> it. Either choice causes a message to be sent to the administrator. When the administrator takes action on the email, a message is sent to the recipient.  <b>NOTE:</b> When a quarantined email is released, it is allowed to pass through the SRX series with a header message that prevents it from being quarantined again, but the attachment is placed inside a password-protected zip file with a text file containing the password that the recipient must use to open the file.</li> </ul>
<i>Email Notifications for End Users</i>	
Learn More Link URL	If you have a corporate web site with further information for users, enter that URL here. If you leave this field blank, this option will not appear to the end user.
Subject	When an email is quarantined, the recipient receives a custom message informing them of their quarantined email. For this custom message, enter a subject indicating a suspicious email sent to them has been quarantined, such as "Malware Detected."
Custom Message	Enter information to help email recipients understand what they should do next.
Custom Link Text	Enter custom text for the Juniper Sky ATP quarantine portal link where recipients can preview quarantined emails and take action on them.

Table 15: Configure Quarantine Malicious Messages (*continued*)

Setting	Guideline
Buttons	<ul style="list-style-type: none"> <li>• Click <b>Preview</b> to view the custom message that will be sent to a recipient when an email is quarantined. Then click <b>Save</b>.</li> <li>• Click <b>Reset</b> to clear all fields without saving.</li> <li>• Click <b>Save</b> if you are satisfied with the configuration.</li> </ul>

Table 16: Configure Deliver with Warning Headers

Setting	Guideline
Action to take	Deliver malicious messages with warning headers added—When you select to deliver a suspicious email with warning headers, you can add headers to emails that most mail servers will recognize and filter into spam or junk folders.
SMTP Headers	<ul style="list-style-type: none"> <li>• X-Distribution (Bulk, Spam)—Use this header for messages that are sent to a large distribution list and are most likely spam. You can also select “Do not add this header.”</li> <li>• X-Spam-Flag—This is a common header added to incoming emails that are possibly spam and should be redirected into spam or junk folders. You can also select “Do not add this header.”</li> <li>• Subject Prefix—You can prepend headers with information for the recipient, such as “Possible Spam.”</li> </ul>
Buttons	<ul style="list-style-type: none"> <li>• Click <b>Reset</b> to clear all fields without saving.</li> <li>• Click <b>OK</b> if you are satisfied with the configuration.</li> </ul>

Table 17: Permit

Setting	Guideline
Action to take	Permit—You can select to permit the message and no further configuration is required.

### Administrators Who Receive Notifications

To send notifications to administrators when emails are quarantined or released from quarantine:

1. Click the + sign to add an administrator.
2. Enter the administrator's email address.
3. Select the **Quarantine Notification** check box to receive those notifications.

4. Select the **Release Notifications** check box to receive those notifications.
5. Click **OK**.

#### RELATED DOCUMENTATION

[Email Management Overview | 65](#)

[SMTP Quarantine Overview: Blocked Emails | 177](#)

[Configuring the SMTP Email Management Policy on the SRX Series Device | 74](#)

## Email Management: Configure IMAP

To access this page, navigate to **Configure > Email Management > IMAP**.

- Read the “[Email Management Overview](#)” on page 65 topic.
  - Decide how malicious emails are handled. For IMAP, the available options are to block or permit email. Unlike SMTP, there is no quarantine option for IMAP and no method for previewing a blocked email.
1. Select **Configure > Email Management > IMAP**.
  2. Based on your selections, configuration options will vary. See the tables below.

Table 18: Configure Block Malicious Messages

Setting	Guideline
Action to take	<ul style="list-style-type: none"> <li>● Permit download of attachments—Allow email attachments, either from all IMAP servers or specific IMAP servers, through to their destination.  <b>NOTE:</b> In Permit mode, black and white lists are not checked. Emails from blacklisted addresses are not sent to the cloud for scanning. They are allowed through to the client.</li> <li>● Block download of attachments—Block email attachments, either from all IMAP servers or specific IMAP servers, from reaching their destination.  <b>NOTE:</b> In Block mode, black and white lists are checked. Emails from blacklisted addresses are blocked. Emails from whitelisted addresses are allowed through to the client.</li> </ul> <p>Recipients can send a request to an administrator to release the email. Enter the email address to which recipients should send a release request.</p> <p><b>NOTE:</b> If a blocked email has multiple recipients, any individual recipient can request to release the email and all recipients will receive it.</p> <p>When you select to block email attachments, in place of the original email, intended recipients receive a custom email you configure with information on the block action. Both the original email and the attachment are stored in the cloud in an encrypted format.</p>
IMAP Server	<ul style="list-style-type: none"> <li>● All IMAP Servers—The permitting or blocking of email attachments applies to all IMAP servers.</li> <li>● Specific IMAP Server—The permitting or blocking of email attachments applies only to IMAP servers with hostnames that you add to a list. A configuration section to add the IMAP server name appears when you select this option.</li> </ul> <p>When you add IMAP servers to the list, it is sent to the SRX Series device to filter emails sent to Juniper Sky ATP for scanning. For emails that are sent for scanning, if the returned score is above the set policy threshold on the SRX, then the email is blocked.</p>
IMAP Servers	<p>Select the <b>Specific IMAP Server</b> option above and click the + sign to add IMAP server hostnames to the list.</p> <p><b>NOTE:</b> You must use the IMAP server hostname and not the IP address.</p>
<i>Email Notifications for End Users</i>	

Table 18: Configure Block Malicious Messages (continued)

Setting	Guideline
Learn More Link URL	If you have a corporate web site with further information for users, enter that URL here. If you leave this field blank, this option will not appear to the end user.
Subject	When an email is blocked, the recipient receives a custom message informing them of their blocked email. For this custom message, enter a subject indicating a suspicious email sent to them has been blocked, such as "Malware Detected."
Custom Message	Enter information to help email recipients understand what they should do next.
Custom Link Text	Enter custom text for the Juniper Sky ATP quarantine portal link where recipients can preview blocked emails and take action on them.
Buttons	<ul style="list-style-type: none"> <li>• Click <b>Preview</b> to view the custom message that will be sent to a recipient when an email is blocked. Then click <b>Save</b>.</li> <li>• Click <b>Reset</b> to clear all fields without saving.</li> <li>• Click <b>Save</b> if you are satisfied with the configuration.</li> </ul>

### Administrators Who Receive Notifications

To send notifications to administrators when emails are blocked or released from quarantine:

1. Click the + sign to add an administrator.
2. Enter the administrator's email address and click **OK**.
3. Once the administrator is created, you can uncheck or check which notification types the administrator will receive.
  - Block Notifications—When this check box is selected, a notification is sent when an email is blocked.
  - Unblock Notifications—When this check box is selected, a notification is sent when a user releases a blocked email.

### RELATED DOCUMENTATION

[IMAP Block Overview | 179](#)

[Email Management Overview | 65](#)



# Email Scanning: SRX Series Device

## IN THIS CHAPTER

- [Configuring the SMTP Email Management Policy on the SRX Series Device | 74](#)
- [Configuring the IMAP Email Management Policy on the SRX Series Device | 80](#)
- [Configuring Reverse Proxy on the SRX Series Device | 88](#)

## Configuring the SMTP Email Management Policy on the SRX Series Device

Unlike file scanning policies where you define an action permit or action block statement, with SMTP email management the action to take is defined in the **Configure > Email Management > SMTP** window. All other actions are defined with CLI commands as before.

Shown below is an example policy with email attachments addressed in profile **profile2**.

```
user@host# show services advanced-anti-malware
...
policy policy1 {
  http {
    inspection-profile default_profile; # Global profile
    action permit;
  }
  smtp {
    inspection-profile profile2; # Profile2 applies to SMTP email
    notification {
      log;
    }
  }
  verdict-threshold 8; # Globally, a score of 8 and above indicate possible
malware
  fallback-options {
    action permit;
    notification {
      log;
    }
  }
}
```



```

    }
  }
  default-notification {
    log;
  }
  whitelist-notification {
    log;
  }
  blacklist-notification {
    log;
  }
  fallback-options {
    action permit; # default is permit and no log.
    notification log;
  }
}
...

```

In the above example, the email profile (profile2) looks like this:

```

user@host> show services advanced-anti-malware profile
Advanced anti-malware inspection profile:
Profile Name: profile2
version: 1443769434
  disabled_file_types:
  {
    application/x-pdfa: [pdfa],
    application/pdf: [pdfa],
    application/mbox: []
  },
  disabled_categories: [java, script, documents, code],
  category_thresholds: [
  {
    category: executable,
    min_size: 512,
    max_size: 1048576
  },
  {
    category: library,
    min_size: 4096,
    max_size: 1048576
  }
  ]

```

The firewall policy is similar to before. The AAMW policy is place in trust to untrust zone. .See the example below.

```

user@host# show security policies from-zone trust to-zone untrust {
  policy p1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          advanced-anti-malware-policy policy1;
          ssl-proxy {
            profile-name ssl-proxy1;
          }
        }
      }
    }
  }
}

```

Shown below is another example, using the **show services advanced-anti-malware policy** CLI command. In this example, emails are quarantined if their attachments are found to contain malware. A verdict score of 8 and above indicates malware.

```

user@root> show services advanced-anti-malware policy policy1
Advanced-anti-malware configuration:
Policy Name: policy1
  Default-notification : No Log
  Whitelist-notification: Log
  Blacklist-notification: Log
  Fallback options:
    Action: permit
    Notification: Log
  Inspection-profile: profile2
  Applications: HTTP
  Verdict-threshold: 8
  Action: block
  Notification: Log
  Protocol: SMTP
  Verdict-threshold: 8

```

```

Action: User-Defined-in-Cloud (quarantine)
Notification: Log
Inspection-profile: profile2

```

Optionally you can configure forward and reverse proxy for server and client protection, respectively. For example, if you are using SMTPS, you may want to configure reverse proxy. For more information on configuring reverse proxy, see [“Configuring Reverse Proxy on the SRX Series Device” on page 88](#).

```

# show services ssl
initiation { # for cloud connection
  profile srx_to_sky_tls_profile_name {
    trusted-ca sky-secintel-ca;
    client-certificate sky-srx-cert;
  }
}
proxy {
  profile ssl-client-protection { # for forward proxy
    root-ca ssl-inspect-ca;
    actions {
      ignore-server-auth-failure;
      log {
        all;
      }
    }
  }
  profile ssl-server-protection { # for reverse proxy
    server-certificate ssl-server-protection;
    actions {
      log {
        all;
      }
    }
  }
}
}

```

Use the **show services advanced-anti-malware statistics** CLI command to view statistical information about email management.

```

user@host> show services advanced-anti-malware statistics
Advanced-anti-malware session statistics:
  Session interested:    3291750

```

```

Session ignored:      52173
Session hit blacklist: 0
Session hit whitelist: 0

```

	Total	HTTP	HTTPS	SMTP	SMTPS
Session active:	52318	0	0	52318	0
Session blocked:	0	0	0	0	0
Session permitted:	1354706	0	0	1354706	0

Advanced-anti-malware file statistics:

	Total	HTTP	HTTPS	SMTP	SMTPS
File submission success:	83134	0	0	83134	0
File submission failure:	9679	0	0	9679	0
File submission not needed:	86104	0	0	86104	0
File verdict meets threshold:	65732	0	0	65732	0
File verdict under threshold:	16223	0	0	16223	0
File fallback blocked:	0	0	0	0	0
File fallback permitted:	4512	0	0	4512	0
File hit submission limit:	0	0	0	0	0

Advanced-anti-malware email statistics:

	Total	SMTP	SMTPS
Email processed:	345794	345794	0
Email permitted:	42722	42722	0
Email tag-and-delivered:	0	0	0
Email quarantined:	9830	9830	0
Email fallback blocked:	0	0	0
Email fallback permitted:	29580	29580	0
Email hit whitelist:	0	0	0
Email hit blacklist:	0	0	0

As before, use the **clear services advanced-anti-malware statistics** CLI command to clear the above statistics when you are troubleshooting.

For debugging purposes, you can also set SMTP trace options.

```
user@host# set services advanced-anti-malware traceoptions flag smtp
```

Before configuring the SMTP threat prevention policy, make sure you have done the following:

- Define the action to take (quarantine or deliver malicious messages) and the end-user email notification in the **Configure > Email Management > SMTP** window.

- (Optional) Create a profile in the **Configure > Device Profiles** window to indicate which email attachment types to scan. Or, you can use the default profile.

The following steps show the minimum configuration. To configure the threat prevention policy for SMTP using the CLI:

1. Create the Juniper Sky ATP policy.

- In this example, the policy name is **smtppolicy1**.

```
user@host# set services advanced-anti-malware policy smtppolicy1
```

- Associate the policy with the SMTP profile. In this example, it is the **default\_profile** profile.

```
user@host# set services advanced-anti-malware policy smtppolicy1
inspection-profile default_profile
```

- Configure your global threshold. If a verdict comes back equal to or higher than this threshold, then it is considered to be malware. In this example, the global threshold is set to 7.

```
user@host# set services advanced-anti-malware policy smtppolicy1
verdict-threshold 7
```

- Apply the SMTP protocol and turn on notification.

```
user@host# set services advanced-anti-malware policy smtppolicy1 smtp
notification log
```

- If the attachment has a verdict less than 7, create log entries.

```
set services advanced-anti-malware policy smtppolicy1 default-notification log
```

- When there is an error condition, send the email to the recipient and create a log entry.

```
set services advanced-anti-malware policy smtppolicy1 fallback-options action
permit
set services advanced-anti-malware policy smtppolicy1 fallback-options
notification log
```

2. Configure the firewall policy to enable the advanced anti-malware application service.

```
[edit security zones]
user@host# set security policies from-zone untrust to-zone trust policy 1 then
  permit application-services advanced-anti-malware smtp-policy1
```

3. In this example, we will configure the reverse proxy.

For reverse proxy:

- Load the CA certificate.
- Load the server certificates and their keys into the SRX Series device certificate repository.

```
user@host> request security pki local-certificate load filename /cf0/cert1.pem
  key /cf0/key1.pem certificate-id server1_cert_id
```

- Attach the server certificate identifier to the SSL proxy profile.

```
user@host# set services ssl proxy profile server-protection-profile
  server-certificate server1_cert_id
```

## Configuring the IMAP Email Management Policy on the SRX Series Device

Unlike file scanning policies where you define an action permit or action block statement, with IMAP email management the action to take is defined in the **Configure > Email Management > IMAP** window. All other actions are defined with CLI commands as before.

**NOTE:** In the IMAP window on Juniper Sky ATP, you can select all IMAP servers or specific IMAP servers and list them. Therefore the IMAP configuration sent to the SRX Series device has a flag called “process\_all\_traffic” which defaults to True, and a list of IMAP servers, which may be empty. In the case where “process\_all\_traffic” is set to True, but there are servers listed in the IMAP server list, then all servers are processed regardless of the server list. If “process\_all\_traffic” is not set to True, only the IMAP servers in the server list are processed.

Shown below is an example policy with email attachments addressed in profile **profile2**.

```

user@host# show services advanced-anti-malware
...
policy policy1 {
    http {
        inspection-profile default_profile; # Global profile
        action permit;
    }
    imap {
        inspection-profile profile2; # Profile2 applies to IMAP email
        notification {
            log;
        }
    }
    verdict-threshold 8; # Globally, a score of 8 and above indicate possible
malware
    fallback-options {
        action permit;
        notification {
            log;
        }
    }
    default-notification {
        log;
    }
    whitelist-notification {
        log;
    }
    blacklist-notification {
        log;
    }
    fallback-options {
        action permit; # default is permit and no log.
        notification log;
    }
}
...

```

In the above example, the email profile (profile2) looks like this:

```

user@host> show services advanced-anti-malware profile
Advanced anti-malware inspection profile:
Profile Name: profile2
version: 1443769434

```

```

disabled_file_types:
{
  application/x-pdfa: [pdfa],
  application/pdf: [pdfa],
  application/mbox: []
},
disabled_categories: [java, script, documents, code],
category_thresholds: [
{
  category: executable,
  min_size: 512,
  max_size: 1048576
},
{
  category: library,
  min_size: 4096,
  max_size: 1048576
}]

```

The firewall policy is similar to before. The AAMW policy is place in trust to untrust zone. See the example below.

```

user@host# show security policies from-zone trust to-zone untrust {
  policy p1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          advanced-anti-malware-policy policy1;
          ssl-proxy {
            profile-name ssl-proxy1;
          }
        }
      }
    }
  }
}

```



Shown below is another example, using the **show services advanced-anti-malware policy** CLI command. In this example, emails are quarantined if their attachments are found to contain malware. A verdict score of 8 and above indicates malware.

```

user@root> show services advanced-anti-malware policy
Advanced-anti-malware configuration:
Policy Name: policy1
  Default-notification   : Log
  Whitelist-notification: No Log
  Blacklist-notification: No Log
  Fallback options:
    Action: permit
    Notification: Log
  Protocol: HTTP
  Verdict-threshold: recommended (7)
    Action: block
    Notification: No Log
    Inspection-profile: default
  Protocol: SMTP
  Verdict-threshold: recommended (7)
    Action: User-Defined-in-Cloud (permit)
    Notification: Log
    Inspection-profile: default
  Protocol: IMAP
  Verdict-threshold: recommended (7)
    Action: User-Defined-in-Cloud (permit)
    Notification: Log
    Inspection-profile: test

```

Optionally you can configure forward and reverse proxy for server and client protection, respectively. For example, if you are using IMAPS, you may want to configure reverse proxy. For more information on configuring reverse proxy, see [“Configuring Reverse Proxy on the SRX Series Device” on page 88](#).

```

# show services ssl
initiation { # for cloud connection
  profile srx_to_sky_tls_profile_name {
    trusted-ca sky-secintel-ca;
    client-certificate sky-srx-cert;
  }
}
proxy {
  profile ssl-client-protection { # for forward proxy

```

```

    root-ca ssl-inspect-ca;
    actions {
        ignore-server-auth-failure;
        log {
            all;
        }
    }
}
profile ssl-server-protection { # for reverse proxy
    server-certificate ssl-server-protection;
    actions {
        log {
            all;
        }
    }
}
}

```

Use the **show services advanced-anti-malware statistics** CLI command to view statistical information about email management.

```

user@host> show services advanced-anti-malware statistics
Advanced-anti-malware session statistics:
Session interested:    3291750
Session ignored:      52173
Session hit blacklist: 0
Session hit whitelist: 0

              Total      HTTP      HTTPS      SMTP      SMTPS      IMAP
IMAPS
Session active:      52318      0        0        52318      0          0
0
Session blocked:    0          0        0          0          0          0
0
Session permitted:  1354706   0        0        1354706   0          0
0

Advanced-anti-malware file statistics:

              Total      HTTP      HTTPS      SMTP      SMTPS
IMAP  IMAPS
File submission success:  83134   0        0        83134     0
0    0
File submission failure:  9679   0        0        9679     0
0    0

```

```

File submission not needed:  86104      0      0      86104      0
0      0
File verdict meets threshold: 65732      0      0      65732      0
0      0
File verdict under threshold: 16223      0      0      16223      0
0      0
File fallback blocked:      0      0      0      0      0
0      0
File fallback permitted:    4512      0      0      4512      0
0      0
File hit submission limit:  0      0      0      0      0
0      0

```

Advanced-anti-malware email statistics:

	Total	SMTP	SMTPS	IMAP	IMAPS
Email processed:	345794	345794	0	0	0
Email permitted:	42722	42722	0	0	0
Email tag-and-delivered:	0	0	0	0	0
Email quarantined:	9830	9830	0	0	0
Email fallback blocked:	0	0	0	0	0
Email fallback permitted:	29580	29580	0	0	0
Email hit whitelist:	0	0	0	0	0
Email hit blacklist:	0	0	0	0	0

As before, use the **clear services advanced-anti-malware statistics** CLI command to clear the above statistics when you are troubleshooting.

For debugging purposes, you can also set IMAP trace options.

```
user@host# set services advanced-anti-malware traceoptions flag imap
```

Before configuring the IMAP threat prevention policy, make sure you have done the following:

- Define the action to take (block or deliver malicious messages) and the end-user email notification in the **Configure > Email Management > IMAP** window.
- (Optional) Create a profile in the **Configure > Device Profiles** window to indicate which email attachment types to scan. Or, you can use the default profile.

The following steps show the minimum configuration. To configure the threat prevention policy for IMAP using the CLI:

1. Create the Juniper Sky ATP policy.

- In this example, the policy name is **imappolicy1**.

```
user@host# set services advanced-anti-malware policy imappolicy1
```

- Associate the policy with the IMAP profile. In this example, it is the **default\_profile** profile.

```
user@host# set services advanced-anti-malware policy imappolicy1
inspection-profile default_profile
```

- Configure your global threshold. If a verdict comes back equal to or higher than this threshold, then it is considered to be malware. In this example, the global threshold is set to 7.

```
user@host# set services advanced-anti-malware policy imappolicy1
verdict-threshold 7
```

- Apply the IMAP protocol and turn on notification.

```
user@host# set services advanced-anti-malware policy imappolicy1 imap
notification log
```

- If the attachment has a verdict less than 7, create log entries.

```
set services advanced-anti-malware policy imappolicy1 default-notification log
```

- When there is an error condition, send the email to the recipient and create a log entry.

```
set services advanced-anti-malware policy imappolicy1 fallback-options action
permit
set services advanced-anti-malware policy imappolicy1 fallback-options
notification log
```

2. Configure the firewall policy to enable the advanced anti-malware application service.

```
[edit security zones]
user@host# set security policies from-zone untrust to-zone trust policy 1 then
permit application-services advanced-anti-malware imappolicy1
```

3. In this example, we will configure the reverse proxy.

For reverse proxy:

- Load the CA certificate.
- Load the server certificates and their keys into the SRX Series device certificate repository.

```
user@host> request security pki local-certificate load filename /cf0/cert1.pem  
key /cf0/key1.pem certificate-id server1_cert_id
```

- Attach the server certificate identifier to the SSL proxy profile.

```
user@host# set services ssl proxy profile server-protection-profile  
server-certificate server1_cert_id
```

## RELATED DOCUMENTATION

[IMAP Block Overview | 179](#)

[Email Management: Configure IMAP | 70](#)

## Configuring Reverse Proxy on the SRX Series Device

Starting with Junos OS Release 15.1X49-D80 and Junos OS Release 17.3R1, the SRX Series device acts as a proxy, so it can downgrade SSL negotiation to RSA. Other changes are shown in [Table 19 on page 88](#).

**Table 19: Comparing Reverse Proxy Before and After Junos OS Release 15.1X49-D80 and 17.3R1**

Feature	Prior to 15.1X49-D80	After 15.1X49-D80 and 17.3R1
Proxy model	Runs only in tap mode Instead of participating in SSL handshake, it listens to the SSL handshake, computes session keys and then decrypts the SSL traffic.	Terminates client SSL on the SRX Series device and initiates a new SSL connection with a server. Decrypts SSL traffic from the client/server and encrypts again (after inspection) before sending to the server/client.
Protocol version	Does not support TLS Version 1.1 and 1.2.	Supports all current protocol versions.
Key exchange methods	Supports RSA.	Supports RSA.
Echo system	Tightly coupled with IDP engine and its detector.	Uses existing SSL forward proxy with TCP proxy underneath.
Security services	Decrypted SSL traffic can be inspected only by IDP.	Just like forward proxy, decrypted SSL traffic is available for all security services.
Ciphers supported	Limited set of ciphers are supported.	All commonly used ciphers are supported.

The remainder of this topic uses the term *SSL proxy* to denote both forward proxy and reverse proxy.

Like forward proxy, reverse proxy requires a profile to be configured at the firewall rule level. In addition, you must also configure server certificates with private keys for reverse proxy. During an SSL handshake, the SSL proxy performs a lookup for a matching server private key in its server private key hash table database. If the lookup is successful, the handshake continues. Otherwise, SSL proxy aborts the handshake. Reverse proxy does not prohibit server certificates. It forwards the actual server certificate/chain as is to the client without modifying it. Intercepting the server certificate occurs only with forward proxy. The following shows example forward and reverse proxy profile configurations.

```
# show services ssl
...
proxy {
    profile ssl-inspect-profile-dut { # For forward proxy. No server cert/key is
needed.
        root-ca ssl-inspect-ca;
```

```

    actions {
        ignore-server-auth-failure;
        log {
            all;
        }
    }
}
profile ssl-1 {
    root-ca ssl-inspect-ca;
    actions {
        ignore-server-auth-failure;
        log {
            all;
        }
    }
}
profile ssl-2 {
    root-ca ssl-inspect-ca;
    actions {
        ignore-server-auth-failure;
        log {
            all;
        }
    }
}
profile ssl-server-protection { # For reverse proxy. No root-ca is needed.
    server-certificate ssl-server-protection;
    actions {
        log {
            all;
        }
    }
}
}
...

```

You must configure either **root-ca** or **server-certificate** in an SSL proxy profile. Otherwise the commit check fails. See [Table 20 on page 90](#).

Table 20: Supported SSL Proxy Configurations

server-certificate configured	root-ca configured	Profile type
No	No	Commit check fails. You must configure either <b>server-certificate</b> or <b>root-ca</b> .
Yes	Yes	Commit check fails. Configuring both <b>server-certificate</b> and <b>root-ca</b> in the same profile is not supported.
No	Yes	Forward proxy
Yes	No	Reverse proxy

Configuring multiple instances of forward and reverse proxy profiles are supported. But for a given firewall policy, only one profile (either a forward or reverse proxy profile) can be configured. Configuring both forward and reverse proxy on the same device is also supported.

You cannot configure the previous reverse proxy implementation with the new reverse proxy implementation for a given firewall policy. If both are configured, you will receive a commit check failure message.

The following are the minimum steps to configure reverse proxy:

1. Load the server certificates and their keys into the SRX Series device certificate repository using the CLI command **request security pki local-certificate load filename *filename* key *key* certificate-id *certificate-id* passphrase *example@1234***. For example:

```
user@host> request security pki local-certificate load filename /cf0/cert1.pem
key /cf0/key1.pem certificate-id server1_cert_id passphrase example@1234
```

2. Attach the server certificate identifier to the SSL Proxy profile using the CLI command **set services ssl proxy profile *profile* server-certificate *certificate-id* passphrase *example@1234***. For example

```
user@host# set services ssl proxy profile server-protection-profile
server-certificate server2_cert_id passphrase example@1234
```

3. Use the **show services ssl** CLI command to verify your configuration. For example:

```
user@host# show services ssl
profile server-protection-profile {
    server-certificate [server1_cert_id , server2_cert_id];
```



```
actions {  
  logs {  
    all;  
  }  
}
```

# File Inspection Profiles

## IN THIS CHAPTER

- File Inspection Profiles Overview | 92
- Creating File Inspection Profiles | 94

## File Inspection Profiles Overview

Access this page from **Configure > File Inspection Management > Profiles**.

Juniper Sky ATP profiles let you define which files to send to the cloud for inspection. You can group types of files to be scanned together (such as .tar, .exe, and .java) under a common name and create multiple profiles based on the content you want scanned. Then enter the profile names on eligible SRX Series devices to apply them.

### Benefits of File Inspection Profiles

- Allows you to create file categories to send to the cloud for scanning rather than having to list every single type of file you want scanned.
- Allows you to configure multiple scanning categories based on file type, adding and removing file types when necessary, increasing or decreasing granularity.

**Table 21: File Category Contents**

Category	Description
Archive	Archive files
Configuration	Configuration files
Document	All document types except PDFs
Executable	Executable binaries
ELF	Executable and Linkable Format (ELF) is a standard file format for executable files, object code, and libraries.

Table 21: File Category Contents (*continued*)

Category	Description
Java	Java applications, archives, and libraries
Library	Dynamic and static libraries and kernel modules
Mobile	Mobile formats
OS package	OS-specific update applications
PDF	PDF, e-mail, and MBOX files
Rich Application	Installable Internet Applications such as Adobe Flash, JavaFX, Microsoft Silverlight
Script	Scripting files

You can also define the maximum file size requirement per each category to send to the cloud. If a file falls outside of the maximum file size limit the file is automatically downloaded to the client system.

**NOTE:** Once the profile is created, use the `set services advanced-anti-malware policy CLI` command to associate it with the Juniper Sky ATP profile.

**NOTE:** If you are using the free or basic model of Juniper Sky ATP, you are limited to only the executable file category.

**NOTE:** The ELF file types support both static analysis and dynamic analysis.

Juniper Sky ATP periodically polls for new and updated content and automatically downloads it to your SRX Series device. There is no need to manually push your profile.

To verify your updates are on your SRX Series devices, enter the following CLI command:

```
show services advanced-anti-malware profile
```

You can compare the version numbers or the contents to verify your profile is current.

**Advanced Anti-malware inspection profile:**

**Profile Name:**default\_profile

**version:** 1443769434

**disabled\_file\_types:**

{ ...

If you do not see your updates, wait a few minutes and try the command again. You might be outside the Juniper Sky ATP polling period.

Once the profile is created, use the **set services advanced-anti-malware policy** CLI command to associate the Juniper Sky ATP profile with the Juniper Sky ATP policy.

## RELATED DOCUMENTATION

[Creating File Inspection Profiles | 94](#)

[Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention | 43](#)

[Removing an SRX Series Device From Juniper Sky Advanced Threat Prevention | 49](#)

*Juniper Sky Advanced Threat Prevention License Types*

## Creating File Inspection Profiles

Use this page to group files under a common, unique name for scanning. By grouping files together into a profile, you can choose file categories to send to the cloud rather than having to list every single type of file you want to scan, such as .tar, .exe, and .java. Once you create your profile name, select one or more check boxes to add file types to be scanned to the profile. Optionally, enter a value limit for the file type in megabytes.

- Review the [“File Inspection Profiles Overview” on page 92](#) topic.
- Note that a default profile, **default\_profile**, is created as part of the initial configuration step. You can modify this default profile, but you cannot delete it.
- If you are using the free or basic model of Juniper Sky Advanced Threat Prevention, you are limited to only the executable file category.

To create a device profile:

1. Select **Configure > File Inspection Management > Profiles**.

2. Click the plus sign (+). Complete the configuration according to the guidelines provided in the table below.
3. Click **OK**.

**Table 22: Device Profile Settings**

Setting	Guideline
Name	Enter a unique name for the profile. This must be a unique string that begins with an alphanumeric character and can include letters, numbers, and underscores; no spaces are allowed; 63-character maximum.
File Categories	<p>You can create several profiles and each profile can contain different options for how each file type is scanned. From the pulldown list for each file type, you can select:</p> <p><b>Do not scan</b> – This file type is not processed for scanning and is always allowed through.</p> <p><b>Hash lookup only</b> – Instead of the file, a sha256 hash of the file is sent for matching against known malware. This may provide a faster result because only a matching of the hash is done and all the file data does not have to be sent. The danger here is that the hash will only match known malware. If the file is a new type of malware that is not known, it will not be recognized as malicious using this method.</p> <p><b>Scan files up to max size</b> – The full content of the file is sent to the cloud for scanning as long as it falls within the set file size limits. If a file exceeds this limit, it is not sent to the cloud for inspection and is transferred to the client. If you do not set the maximum file size, a default of 32 MB is used.</p>

**NOTE:** You can create up to 32 profiles.

**NOTE:** Juniper Sky ATP periodically polls for new and updated content and automatically downloads it to your SRX Series device. There is no need to manually push your profile.

[RELATED DOCUMENTATION](#)

[Enabling Third Party Threat Feeds | 110](#)

---

[File Inspection Profiles Overview | 92](#)

---

*Juniper Sky Advanced Threat Prevention License Types*

# Adaptive Threat Profiling

## IN THIS CHAPTER

- [Adaptive Threat Profiling Overview | 97](#)
- [Create an Adaptive Threat Profiling Feed | 108](#)

## Adaptive Threat Profiling Overview

### IN THIS SECTION

- [Overview | 97](#)
- [Configure Adaptive Threat Profiling | 99](#)
- [Deploy Adaptive Threat Profiling | 101](#)
- [Use Case Examples | 103](#)

### Overview

Juniper Sky ATP Adaptive Threat Profiling allows SRX Series devices to generate, propagate, and consume threat feeds based on their own advanced detection and policy-match events.

This feature allows you to configure security or IDP policies that, when matched, inject the source or destination IP address into a threat feed, which can be leveraged by other devices as a dynamic-address-group (DAG). While this feature is focused on tracking and mitigating threat actors within a network, you can also use it for non-threat related activities, such as device classification.

With adaptive threat profiling, the Juniper Sky ATP service acts as a feed-aggregator and consolidates feeds from SRX across your enterprise and shares the deduplicated results back to all SRX series devices in the realm at regular intervals. SRX Series devices can then use these feeds to perform further actions against the traffic.

**NOTE:** This feature requires a SecIntel License (Premium model) to function. Additional detection capabilities may require AppID, IDP, and Enhanced Web Filtering licenses to be added to your device if not already present. For information on other licensed features, see *Juniper Sky Advanced Threat Prevention License Types*.

### Benefits of adaptive threat profiling

- Enables new deployment architectures, whereby low cost SRX Series devices can be deployed as sensors throughout the network on Tap ports, identifying and sharing intelligence to in-line devices for real-time enforcement.
- Allows administrators near-infinite adaptability to changing threats and network conditions. Security policies can be staged with adaptive threat profiling feeds, which automatically populate with entries in the event of an intrusion or malware outbreak.
- Provides the ability to perform endpoint classification. You can classify endpoints based on network behavior and/or deep packet inspection (DPI) results. For example, you can leverage AppID, Web-Filtering, or IDP to place hosts that communicate with Ubuntu's update servers into a dynamic-address-group that can be used to control Ubuntu-Server behavior on your network.

Access this page from **Configure > Adaptive Threat Profiling**.

**Table 23: Adaptive Threat Profiling**

Field	Guideline
Feed Name	Name of the adaptive threat profiling feed.
Items	Number of entries in the feed.
Feed Type	Content type of the feed.  <b>NOTE:</b> Currently, this feature only supports IP addresses.
Time to Live (days)	Defines how long an entry will "live" inside the feed. Once the TTL is reached, the entry is removed automatically.

**NOTE:**

- The feeds can only be used as dynamic-address groups (DAG) /IP filter.

You can perform the following tasks from this page:



- Add a new feed—See “[Create an Adaptive Threat Profiling Feed](#)” on page 108.
- Modify a feed—Select a feed and click the edit icon (pencil). The Edit <feed-name> page appears, displaying the same fields that were presented when you create a feed. Modify the fields as needed. Click **OK** to save your changes.

**NOTE:** You cannot edit the feed name and feed type.

- Delete a feed—Select a feed and click the delete icon in the title bar. A pop-up requesting confirmation for the deletion appears. Click **Yes** to confirm that you want to delete the feed.
- Filter or Search for a feed. Click the filter icon. Enter partial text or full text of the keyword in the search bar and click the search button or press **Enter**. The search results are displayed. You can also filter by feed type and Time to Live (days).
- View detailed information about a feed—Click on a feed name to view the following information:
  - Feed Items—Lists all the IP addresses that are associated with the feed. To exclude an IP address from the feed, select the IP address and click **Add to Excluded Items**.
  - Excluded Items—Lists all the IP addresses that are excluded from the feed. To remove an IP address for the excluded items list, select the IP address and click the Delete icon.

## Configure Adaptive Threat Profiling

An SRX Series device that has already been enrolled with Juniper Sky ATP should include all the necessary configuration to begin leveraging adaptive threat profiling.

To begin, validate that the device already contains a URL for security-intelligence.

1. Check the URL for the feed server.

Your output should look similar to the following:

```
show services security-intelligence url
https://cloudfeeds.sky.junipersecurity.net/api/manifest.xml
```

**NOTE:** If the URL is not present in the configuration, try re-enrolling the device in Juniper Sky ATP. See [“Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention” on page 43.](#)

2. Create an adaptive threat profiling feed in Juniper Sky ATP. Log into Juniper Sky ATP UI, select **Configure > Adaptive Threat Profiling**. The Adaptive Threat Profiling page appears as shown in [Figure 18 on page 100](#). In this example, we will use the feed name **High\_Risk\_Users** with a time-to-live (TTL) of seven days.

Figure 18: Add New Feed

## Add New Feed ?

Feed Name\* ?

Type ?

 ▼

Time To Live\* ?

 ▲  
▼

Cancel

OK

3. Click **OK** to save changes. For more information, see [“Create an Adaptive Threat Profiling Feed” on page 108.](#)
4. Ensure that the feed has been downloaded by your SRX Series device. This is done automatically at regular intervals but can take a few minutes. A manual download of the security-intelligence database can speed up this process, if necessary.

```
> request services security-intelligence download

> request services security-intelligence download status |match High_Risk_Users

Feed High_Risk_Users (20200615.1) root-logical-system of category SecProfiling
download succeeded.
```

## Deploy Adaptive Threat Profiling

You can deploy adaptive threat profiling on the SRX Series devices in the following ways:

- As a detection solution
- As an enforcement solution
- As both detection and enforcement solution

To use adaptive threat profiling to detect threats, you can define adaptive threat profiling actions in the following locations:

1. Within the security policy on deny, reject, and permit rules, where you can add the source and/or destination address of the flow to a feed of your choice.

```
[edit security policies global policy Threat_Profiling]
admin@vSRX# set then permit application-services security-intelligence ?
Possible completions:
> add-destination-ip-to-feed  Add Destination IP to Feed
> add-source-ip-to-feed     Add Source IP to Feed
```

2. Within an IDP Policy as an application-service that adds the origin of the exploit (the attacker) or the target of the exploit to a feed of your choice.

```
[edit security idp idp-policy Threat_Profiling rulebase-ips rule Scanners]
admin@vSRX# set then application-services security-intelligence ?
```

Possible completions:

```
add-attacker-ip-to-feed Specify the desired feed-name
add-target-ip-to-feed Specify the desired feed-name
```

To take effect, you must apply the IDP policy to a traditional policy or unified policy.

```
[edit security policies global policy Threat_Profiling]
admin@vSRX# set then permit application-services idp-policy Threat_?
Possible completions:
Threat_Profiling [security idp idp-policy]
```

Once the feed is created, it can then be referenced as a dynamic address group within a security policy as the source-address or destination-address match criteria.

In the following example, we have created a rule which allows authenticated users access to the Enterprise's **Crown Jewels**, but are excluding any source-addresses that are part of the **High\_Risk\_Users** dynamic address group (sourced from the threat feed of the same name).

```
[edit security policies global policy Access_To_Crown_Jewels]
admin@vSRX# show
match {
    source-address High_Risk_Users;
    destination-address Crown_Jewels;
    source-address-excluded;
    source-identity authenticated-user;
    dynamic-application any;
}
then {
    permit;
    log {
        session-close;
    }
}
```

Use the following command to view the feed summary and status:

**show services security-intelligence sec-profiling-feed status**

```
show services security-intelligence sec-profiling-feed status Category name
:SecProfiling
Feed name :High_Risk_Users
```

```

Feed type      :IP
Last post time :2020-02-06 10:54:10 PST Last post status code:200
Last post status :succeeded

```

### show security dynamic-address category-name SecProfiling

```

show security dynamic-address category-name SecProfiling
No.      IP-start      IP-end      Feed      Address
1        10.1.1.100    10.1.1.100  High_Risk_Users  High_Risk_Users
2        192.168.0.10  192.168.0.10  High_Risk_Users  High_Risk_Users
3        192.168.0.88  192.168.0.88  High_Risk_Users  High_Risk_Users

```

**NOTE:** Dynamic-address entries will only be displayed by this command if the feed name being referenced (High\_Risk\_Users in the example), has been used as a source or destination address in a security policy.

Feed contents can always be viewed in the Juniper Sky ATP portal, regardless of their state on the SRX Series devices.

## Use Case Examples

### IN THIS SECTION

- [Threat Detection Use Case | 103](#)
- [Asset Classification Use Case | 107](#)

### *Threat Detection Use Case*

In this example, we will continue with the definition of the High\_Risk\_Users use case, with the goal of identifying any unusual activity which may suggest an endpoint has been compromised.

1. Create a policy that detects the usage of The Onion Router (TOR), Peer-to-Peer (P2P), and Anonymizers / Proxies and add the source IP address of these to the High\_Risk\_Users feed.

```
[edit security policies global policy Unwanted_Applications]
admin@vSRX# show
match {
    source-address any;
    destination-address any;
    application junos-defaults;
    dynamic-application [ junos:p2p junos:web:proxy junos:TOR junos:TOR2WEB ];
}
then {
    deny {
        application-services {
            security-intelligence {
                add-source-ip-to-feed {
                    High_Risk_Users;
                }
            }
        }
    }
    log {
        session-close;
    }
}
```

2. Create a second policy that looks for communication with known malicious sites and malware Command-and-Control (C2) infrastructure as well as newly registered domains and adds it to High\_Risk\_Users feed.

```
[edit security policies global policy URL-C2-Detection]
admin@vSRX# show
match {
    source-address any;
    destination-address any;
    application [ junos-http junos-https ];
    dynamic-application any;
    url-category [ Enhanced_Compromised_Websites Enhanced_Emerging_Exploits
Enhanced_Keyloggers Enhanced_Malicious_Embedded_Link
Enhanced_Malicious_Embedded_iFrame Enhanced_Malicious_Web_Sites
Enhanced_Newly_Registered_Websites ];
}
then {
    deny {
        application-services {
```

```

        security-intelligence {
            add-source-ip-to-feed {
                High_Risk_Users;
            }
        }
    }
}
log {
    session-close;
}
}
}
}

```

### 3. Create an IDP policy that identifies unusual scanning activity and brute-force attempts.

```

[edit security idp idp-policy Threat_Profiling rulebase-ips rule Scanners]
admin@vSRX# show
match {
    attacks {
        predefined-attacks [ SCAN:NMAP:FINGERPRINT SCAN:METASPLOIT:SMB-ACTIVE
SCAN:METASPLOIT:LSASS SMB:AUDIT:BRUTE-LOGIN APP:RDP-BRUTE-FORCE
FTP:PASSWORD:BRUTE-FORCE LDAP:FAILED:BRUTE-FORCE SSH:BRUTE-LOGIN ];
    }
}
then {
    action {
        drop-connection;
    }
    notification {
        log-attacks;
        packet-log;
    }
    application-services {
        security-intelligence {
            add-attacker-ip-to-feed High_Risk_Users;
        }
    }
}
}
}

```

**NOTE:** This is an example of a safe policy to deploy on a Tap-based SRX sensor. The example does not make sense to deploy on an in-line device due to the permissive nature of the rule. In production, we recommend being more restrictive.

4. Apply the IDP rulebase to a security policy to take effect.

```
[edit security policies global policy IDP_Threat_Profiling]
admin@vSRX# show
match {
    source-address any;
    destination-address any;
    application any;
    dynamic-application any;
}
then {
    permit {
        application-services {
            idp-policy Threat_Profiling;
        }
    }
    log {
        session-close;
    }
}
```

5. Create a simple rule at the top of the rule-base which drops any traffic from hosts within the High\_Risk\_Users threat feed.

```
[edit security policies global policy Drop_Risky_Users]
admin@vSRX# show
match {
    source-address High_Risk_Users;
    destination-address any;
    application any;
}
then {
    deny;
    log {
        session-close;
    }
}
```



```

    }
}

```

### **Asset Classification Use Case**

In this example, we will leverage AppID to identify Ubuntu and RedHat servers in an environment and add them to feed for use by other devices.

As many legacy devices lack the compute power required to enable Deep-Packet Inspection (DPI), adaptive threat profiling can provide you a flexible way in which you can share DPI classification results between newer and older platforms in your environment.

Create a security policy that identifies Advanced Packaging Tool (APT) and Yellowdog Updater, Modified (YUM) communication with Ubuntu and RedHat Update servers:

```

[edit security policies global policy Linux_Servers]
admin@vSRX# show
match {
    source-address any;
    destination-address any;
    application junos-defaults;
    dynamic-application [ junos:UBUNTU junos:REDHAT-UPDATE ];
}
then {
    permit {
        application-services {
            security-intelligence {
                add-source-ip-to-feed {
                    Linux_Servers;
                }
            }
        }
    }
}
}

```

### RELATED DOCUMENTATION

| [Create an Adaptive Threat Profiling Feed](#) | 108

## Create an Adaptive Threat Profiling Feed

Use this page to add a new adaptive threat profiling feed.

Review the [“Adaptive Threat Profiling Overview” on page 97](#) topic.

To add a new adaptive threat profiling feed:

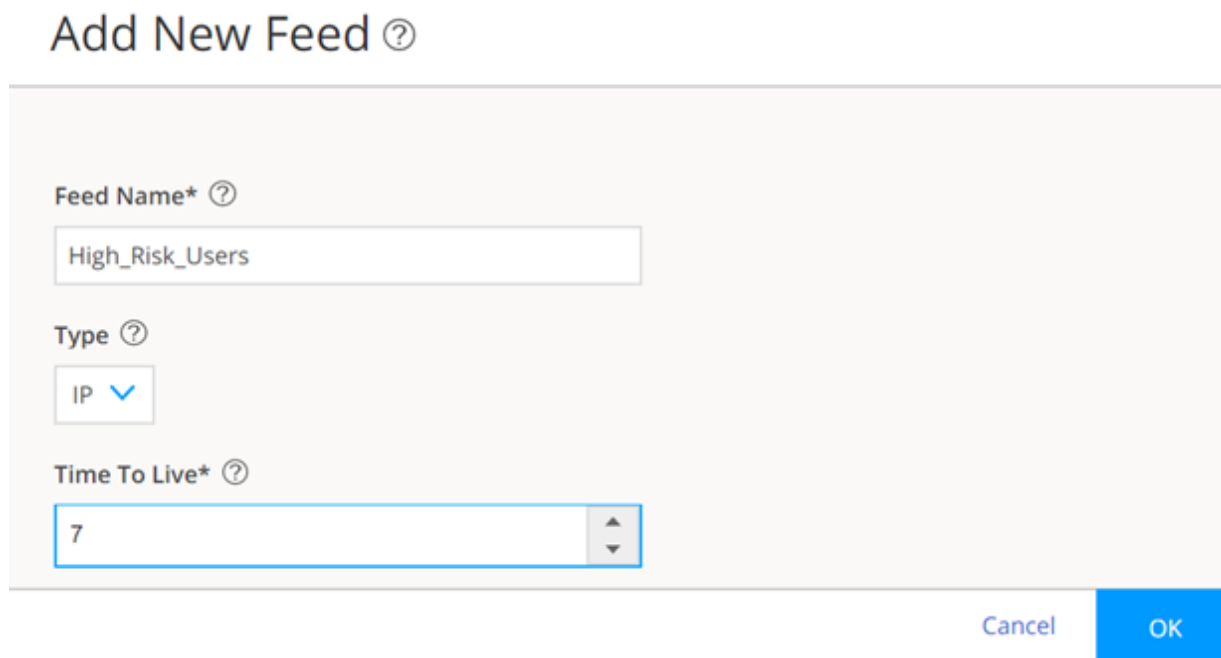
1. Select **Configure > Adaptive Threat Profiling**.

The Adaptive Threat Profiling page appears.

2. Click the plus sign (+).

The Add New Feed page appears as shown in [Figure 19 on page 108](#).

Figure 19: Add New Feed Settings



**Add New Feed** ?

Feed Name\* ?  
High\_Risk\_Users

Type ?  
IP ▾

Time To Live\* ?  
7

Cancel OK

3. Complete the configuration according to the guidelines provided in the [Table 24 on page 109](#).

4. Click **OK** to save the changes.

Table 24: Add New Feed Settings

Setting	Guideline
Feed Name	Enter a unique name for the threat feed. The feed name must begin with an alpha-numeric character and can include letters, numbers, and underscores; no spaces are allowed. The length is 8–63 characters.
Type	Select the content type of the feed.  <b>NOTE:</b> Currently, this feature only supports IP addresses.
Time to Live	Enter the number of days for the required feed entry to be active. After the feed entry crosses the time to live (TTL) value, the feed entry is automatically removed. The available range is 1–365 days.

**NOTE:**

- You can create a maximum of 32 feeds.
- After you create a feed, the same feed will be available for configuration on the Junos CLI.

**RELATED DOCUMENTATION**

[Adaptive Threat Profiling Overview](#) | 97

# Third Party Threat Feeds

## IN THIS CHAPTER

- [Enabling Third Party Threat Feeds | 110](#)

## Enabling Third Party Threat Feeds

Using this page, you can enable external, third party feeds for integration with Juniper Sky ATP.

**NOTE:** There is a limit to the number of feeds you can have. When you enable feeds from this page, they count toward your limit of 29 feeds. This is applicable if you are injecting additional feeds using the available open API.

Information to know if you are enabling external feeds:

- If a hit is detected on an enabled external feed, this event appears under **Monitor > C&C Servers** with a threat level of 10.
- On enrolled SRX Series devices, you can configure policies with permit or block actions for each feed. Note that C&C and Infected Host feeds require an enabled Security Intelligence policy on the SRX Series device in order to work.
- External feeds are updated once every 24 hours.



**WARNING:** Understand that these are open source feeds managed by third parties and determining the accuracy of the feed is left up to the Juniper Sky ATP administrator. Juniper will not investigate false positives generated by these feeds.



**WARNING:** Configured SRX Series policies will block malicious IP addresses based on enabled third party feeds, but these events do not affect host threat scores. Only events from Juniper Sky ATP feeds affect host threat scores.

To enable the available feeds, do the following:

1. Navigate to **Configure > Third Party Feeds**.
2. For each feed, select the check box to enable the feed. Refer to the guidelines in [Table 25 on page 111](#).

Click the **Go to feed site** link to view feed information, including the contents of the feed.

**Table 25: Third Party Feeds**

Field	Guidelines
<b>IP Filter Feed</b>	
office365	Select the check box to enable office365 IP filter feed as a third party feed. The office365 IP filter feed is an up-to-date list of published IP addresses for Office 365 service endpoints which you can use in security policies. This feed works differently from others on this page and requires certain configuration parameters, including a pre-defined name of "ipfilter_office365". See more instructions at the bottom of this page, including usage of the <b>set security dynamic-address</b> command for using this feed.
<b>Command and Control Feeds</b>	
<b>IP Feed</b>	
Malware Domain List	Select the check box to enable malware domain list feed as third party feeds.
Block List	Select the check box to enable block list feeds as third party feeds.
DShield	Select the check box to enable DShield feeds as third part feeds.
Tor	Select the check box to enable tor feeds as third part feeds.
<b>URL Feeds</b>	
URLhaus URL Threat Feed	Select the check box to enable URLhaus feed as third party feeds. URLhaus is a threat intelligence feed that shares malicious URLs that are used for malware distribution.

Table 25: Third Party Feeds (continued)

Field	Guidelines
Open Phish	Select the check box to enable OpenPhish feed as third party feeds. OpenPhish is a fully automated self-contained platform for phishing intelligence. It identifies phishing sites and performs intelligence analysis in real time without human intervention and without using any external resources, such as blacklists. For malware inspection, SecIntel will analyze traffic using URLs in this feed.

**NOTE:**

- Starting in Junos OS Release 19.4R1, third party URL feeds are supported on Juniper Sky ATP.
- Since Ransomware Tracker is deprecated, ransomware tracker IP feeds are not supported on Juniper Sky ATP. If you had enabled this feed earlier, you might stop receiving these feeds.

3. Like other C&C and infected host feeds, enabled third party feeds require a security intelligence policy on the SRX Series device in order to work. Example commands are provided here. Please refer to the [Juniper Sky Advanced Threat Prevention CLI Reference Guide](#) for more information.

- On the SRX Series Device: Configure a Security Intelligence Profile

```

set services security-intelligence profile secintel_profile category CC
set services security-intelligence profile secintel_profile rule secintel_rule match threat-level 10
set services security-intelligence profile secintel_profile rule secintel_rule match threat-level 9
set services security-intelligence profile secintel_profile rule secintel_rule then action block close
set services security-intelligence profile secintel_profile rule secintel_rule then log
set services security-intelligence profile secintel_profile default-rule then action permit
set services security-intelligence profile secintel_profile default-rule then log
set services security-intelligence profile ih_profile category Infected-Hosts
set services security-intelligence profile ih_profile rule ih_rule match threat-level 10
set services security-intelligence profile ih_profile rule ih_rule then action block close
set services security-intelligence profile ih_profile rule ih_rule then log
set services security-intelligence policy secintel_policy Infected-Hosts ih_profile
set services security-intelligence policy secintel_policy CC secintel_profile

```

4. The security intelligence policy must also be added to an SRX Series device policy.

- On the SRX Series Device: Configure a Security Policy (Enter the following commands to create a security policy on the SRX Series device for the inspection profiles.)

**set security policies from-zone trust to-zone untrust policy 1 match source-address any**

**set security policies from-zone trust to-zone untrust policy 1 match destination-address any**

**set security policies from-zone trust to-zone untrust policy 1 match application any**

**set security policies from-zone trust to-zone untrust policy 1 then permit application-services  
ssl-proxy profile-name ssl-inspect-profile-dut**

**set security policies from-zone trust to-zone untrust policy 1 then permit application-services  
security-intelligence-policy secintel\_policy**

For more information on configuring the SRX Series with Juniper Sky ATP using the available CLI commands, refer to the [Juniper Sky Advanced Threat Prevention CLI Reference Guide](#).

### Using the office365 Feed

1. Enable the **Using the office365 Feed** check box in Juniper Sky ATP to push Microsoft Office 365 services endpoint information (IP addresses) to the SRX Series device. The office365 feed works differently from other feeds on this page and requires certain configuration parameters, including a pre-defined name of "ipfilter\_office365".
2. After you enable the check box, you must create a dynamic address object on the SRX Series device that refers to the ipfilter\_office365 feed as follows:
  - **set security dynamic-address address-name office365 profile category IPFilter feed ipfilter\_office365**

**NOTE:** A security policy can then reference the dynamic address entry name ('office365' in this example) in the source or destination address.

A sample security policy is as follows:

```
policy o365 {
  match {
    source-address any;
    destination-address office365;
    application any;
  }
  then {
    deny;
    log {
      session-init;
    }
  }
}
```

```

}
}
}

```

Use the following command to verify the office365 feed has been pushed to the SRX Series device. (**Update status** should display **Store succeeded.**)

- **show services security-intelligence category summary**

```

Category name      :IPFilter
Status             :Enable
Description        :IPFilter data
Update interval    :3600s
TTL                :3456000s
Feed name          :ipfilter_office365
Version           :20180405.1
Objects number     :934
Create time        :2018-04-16 07:05:33 PDT
Update time        :2018-04-16 12:17:47 PDT
Update status      :Store succeeded
Expired            :No
Options            :N/A

```

Use the following command to show all the individual feeds under IPFILTER.

- **show security dynamic-address category-name IPFilter**

No.	IP-start	IP-end	Feed	Address
1	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365	office365
2	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365	office365
3	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365	office365
4	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365	office365
5	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365	office365
6	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365	office365
7	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365	office365



8	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365 office365
9	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365 office365
10	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365 office365
11	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365 office365
12	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365 office365
13	x.x.x.x	x.x.x.x	IPFilter/ipfilter_office365 office365

## RELATED DOCUMENTATION

[Hosts Overview | 137](#)

[Host Details | 140](#)

# Global Configurations

## IN THIS CHAPTER

- Global Configuration for Infected Hosts | 116
- Configuring Threat Intelligence Sharing | 119
- Configuring Trusted Proxy Servers | 121
- Realm Overview | 122
- Realm Management | 124
- Tenant Systems: Security-Intelligence and Anti-Malware Policies | 126

## Global Configuration for Infected Hosts

### Threat Level Threshold

Set the global threat level to block infected hosts. When a host is found to be compromised, it is assigned a threat level. Based on the global threat level you set here, 1-10 with 10 being the highest threat, compromised hosts with the set threat level and above are added to the infected hosts lists and can subsequently be blocked by policies configured on the SRX Series device. See [“Hosts Overview” on page 137](#) and [“Configuring the SRX Series Devices to Block Infected Hosts” on page 149](#) for more information.

You can configure Juniper Sky ATP to send e-mails when certain threat levels are reached for infected hosts. For example, you can send e-mails to an IT department when thresholds of 5 are met and send e-mails to an escalation department when thresholds of 9 are met.

You can send e-mails to any account; you are not restricted to administrator e-mails defined in the Users window. The Web UI does not verify if an e-mail account is valid.

## Configure Threat Level Threshold and Email Alerts

### Benefits of the Global Infected Hosts Alerts

- Email alerts for infected hosts call immediate attention to administrators when a possible network security issue arises.
- Email alerts can be configured for only specific administrators and not all users of the web portal, targeting alerts more narrowly.

1. Select **Configure > Global Configuration > Infected Hosts**.
2. (Premium licenses only) Set the default threat level threshold.
3. Click the plus sign to create e-mail alerts, or click the pencil icon to edit existing ones. Configure the fields described in the table below.
4. Click **OK**.

**Table 26: Email alerts for infected hosts fields**

Setting	Guideline
Threat Level	Select a threat level between 1 and 10. When this level is reached, an e-mail is sent to the address you provided.
E-mail	Enter an e-mail address.

### Automatically Expire Blocked Hosts

When a host is marked as infected and added to the infected hosts feed, it is blocked from the network by policies configured on the SRX Series device. There are options for unblocking individual hosts on the **Host Details** page in the Juniper Sky ATP Web Portal. See [“Hosts Overview” on page 137](#) for information. If you want to unblock multiple host IP addresses based on time period and threat level, you would use the **Automatically Expire Blocked Hosts** feature on the **Global Configuration > Infected Hosts** page in the Web Portal.

From the Global Infected Hosts page, you can set infected hosts to expire after a configured time based on a minimum and maximum threat level. Once the time period is reached, blocked IP addresses are no longer marked as infected and therefore no longer blocked.

One example of when you might use this feature is if you are using DHCP addressing and reallocating addresses on a set schedule. In that case, you may want to set an expiration time for infected hosts (based on IP address lease times), after which addresses are no longer marked as infected.

## Configure Automatic Expiration of Infected Hosts

1. Select **Configure > Global Configuration > Infected Hosts**.
2. (System Administrators and Operators only) Enable **Automatically Expire Blocked Hosts** and select one of the following:

- **Unblock all hosts**
- **Unblock a range of hosts**—Enter a range of IPv4 or IPv6 addresses.

Any of the following IPv4 formats are valid: **1.2.3.4/30**, or **1.2.3.4-1.2.3.6**

Any of the following IPv6 formats are valid: **1111::1-1111::9**, or **1111:1::0/64**

**NOTE:** No more than a block of /16 IPv4 addresses and /48 IPv6 addresses are accepted. For example, **10.0.0.0-10.0.255.255** is valid, but **10.0.0.0-10.1.0.0** is not.

**Bitmasks:** The maximum amount of IP addresses covered by bitmask in a subnet record for IPv4 is 16 and for IPv6 is 48. For example, **10.0.0.0/15** and **1234::/47** are not valid. CIDR notation is also accepted.

3. For both **Unblock all hosts** or **Unblock a range of hosts**, you must also set expiration intervals and threat levels. Click the plus + sign to create a new entry and set the following in the **Unblocked Expiration Intervals** table.

**Table 27: Unblock expiration interval fields**

Setting	Guideline
Set the Minimum Threat Level	Click the table entry under <b>Minimum Threat Level</b> to access a pulldown menu. Select a minimum threat level (1-10). The level you select is included in the minimum setting.
Set the Maximum Threat Level	Click the table entry under <b>Maximum Threat Level</b> to access a pulldown menu. Select a maximum threat level (1-10). The level you select is included in the maximum setting.
Set the Hours to Unblock	Click the table entry under <b>Hours to Unblock</b> . You can select Never, 6, 12, 18, or 24 hours. After the set amount of hours, the infected label expires and the hosts are no longer blocked.

Table 27: Unblock expiration interval fields (*continued*)

Setting	Guideline
<p>For example, if you set the minimum at 6 and the maximum at 8 with hours to unblock as 24, the following would occur. All infected hosts with a threat level of 6 and above and 8 and below would expire after 24 hours.</p> <p><b>NOTE:</b> You can create multiple entries in this table, setting different expiration times for different threat levels.</p> <p>Once unblock settings are entered in the table, you can use the table to change existing settings or to delete settings.</p>	

4. You must click **Save** or your settings are lost.

## RELATED DOCUMENTATION

[Configuring the SRX Series Devices to Block Infected Hosts | 149](#)

[Hosts Overview | 137](#)

[Modifying My Profile | 210](#)

[Creating and Editing User Profiles | 211](#)

## Configuring Threat Intelligence Sharing

Using the TAXII service, Juniper Sky ATP can contribute to STIX reports by sharing the threat intelligence it gathers from file scanning. Juniper Sky ATP also uses threat information from STIX reports as well as other sources for threat prevention. See [“HTTP File Download Details” on page 166](#) for more information on STIX reports.

- STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties.
- STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing.
- If you enable TAXII (it is disabled by default), you can limit who has access to your shared threat information by creating an application token. See [“Creating Application Tokens” on page 213](#).

To enable and configure threat intelligence sharing, do the following:

1. Select **Configure > Global Configuration > Threat Intelligence Sharing**.

2. Move the knob to the right to **Enable TAXII**.
3. Move the sidebar to designate a file sharing threshold. Only files that meet or exceed the set threshold will be used in STIX reports. The default is threat level 6 or higher.

**NOTE:** You can limit who has access to your information by creating an application token. See. "[Creating Application Tokens](#)" on page 213.

**Table 28: Additional Information**

TAXII URLs and Services	Description
Discovery URL	<p>Used by the TAXII client to discover available TAXII Services. The command to initiate a TAXII request is: <b>taxii-discovery</b></p> <p><b>NOTE:</b> Refer to the TAXII documentation for information on additional commands. <a href="http://taxiiproject.github.io/documentation/">http://taxiiproject.github.io/documentation/</a></p> <p>Juniper Sky ATP Discovery URLs are:</p> <p>US Region: <a href="https://taxii.sky.junipersecurity.net/services/discovery">https://taxii.sky.junipersecurity.net/services/discovery</a></p> <p>EU Region: <a href="https://taxii-eu.sky.junipersecurity.net/services/discovery">https://taxii-eu.sky.junipersecurity.net/services/discovery</a></p> <p>APAC Region: <a href="https://taxii-apac.sky.junipersecurity.net/services/discovery">https://taxii-apac.sky.junipersecurity.net/services/discovery</a></p> <p>Canada: <a href="https://taxii-canada.sky.junipersecurity.net/services/discovery">https://taxii-canada.sky.junipersecurity.net/services/discovery</a></p>
<p>At this time, there are two services supported by Juniper Sky ATP on the TAXII server.</p>	
Collection Management	<p>Used by the TAXII client to request information about available data collections.</p> <p>Juniper Sky ATP Collection Management URLs are:</p> <p>US Region: <a href="https://taxii.sky.junipersecurity.net/services/collection-management">https://taxii.sky.junipersecurity.net/services/collection-management</a></p> <p>EU Region: <a href="https://taxii-eu.sky.junipersecurity.net/services/collection-management">https://taxii-eu.sky.junipersecurity.net/services/collection-management</a></p> <p>APAC Region: <a href="https://taxii-apac.sky.junipersecurity.net/services/collection-management">https://taxii-apac.sky.junipersecurity.net/services/collection-management</a></p> <p>Canada: <a href="https://taxii-canada.sky.junipersecurity.net/services/collection-management">https://taxii-canada.sky.junipersecurity.net/services/collection-management</a></p>

Table 28: Additional Information (continued)

TAXII URLs and Services	Description
Poll URL	<p>Used by the TAXII client to poll for STIX files - looking for malware that has been identified on the network.</p> <p>Juniper Sky ATP Polling URLs are:</p> <p>US Region: <a href="https://taxii.sky.junipersecurity.net/services/poll">https://taxii.sky.junipersecurity.net/services/poll</a></p> <p>EU Region: <a href="https://taxii-eu.sky.junipersecurity.net/services/poll">https://taxii-eu.sky.junipersecurity.net/services/poll</a></p> <p>APAC Region: <a href="https://taxii-apac.sky.junipersecurity.net/services/poll">https://taxii-apac.sky.junipersecurity.net/services/poll</a></p> <p>Canada: <a href="https://taxii-canada.sky.junipersecurity.net/services/poll">https://taxii-canada.sky.junipersecurity.net/services/poll</a></p>

## RELATED DOCUMENTATION

[HTTP File Download Details](#) | 166

[Creating Application Tokens](#) | 213

## Configuring Trusted Proxy Servers

Use this page to add trusted proxy server IP addresses to Juniper Sky ATP. This feature is optional

**NOTE:** Support starting in Junos OS 17.4R1.

Access this page from **Configure > Global Configuration > Proxy Servers**.

When there is a proxy server between users on the network and a firewall, the firewall might see the proxy server IP address as the source of an HTTP or HTTPS request instead of the actual address of the user making the request.

With this in mind, X-Forwarded-For (XFF) is a standard header added to packets by a proxy server that includes the real IP address of the client making the request. Therefore, if you add trusted proxy servers IP addresses to the list in Juniper Sky ATP, by matching this list with the IP addresses in the HTTP header (X-Forwarded-For field) for requests sent from the SRX Series devices, Juniper Sky ATP can determine the originating IP address.

**NOTE:** X-Forwarded-For (XFF) only applies to HTTP or HTTPS traffic, and only if the proxy server supports the XFF header.

To add trusted proxy servers to the list, do the following:

1. Navigate to **Configure > Global Configuration > Proxy Servers**.
2. Click the + sign.
3. Enter the IP address of the proxy server in the available field.
4. Click **OK**.

#### RELATED DOCUMENTATION

[Hosts Overview | 137](#)

[Compromised Hosts: More Information | 142](#)

## Realm Overview

### Realms and Tenant Systems

Realms are a way to partition configurations and apply different security policies to SRX Series devices and tenant systems. When you associate a device or tenant system with a realm in Juniper Sky ATP, that device receives the threat management features configured for the realm. You can also provide different levels of administrator access to individual realms.



**WARNING:** Unlike physical devices, which automatically make submissions to the realm they are enrolled in, tenant system submissions are ignored until they are explicitly associated with a realm using the Realm Management page in the Juniper Sky ATP Web UI. See [“Realm Management” on page 124](#) for those instructions.

For example, if a managed security service provider (MSSP) partitions customers by realm and then associates all SRX Series tenant systems for an individual customer with their assigned realm, that MSSP



can deliver targeted threat prevention policies to multiple customers while allowing administrators to easily switch between realms for monitoring purposes.

Alternatively, if customers are partitioned by tenant system, an MSSP could configure a one-to-one mapping of realms to tenant systems for each customer.

For monitoring, each tenant system is included in log file events and different administrators can be given varying levels of access to each realm. The main realm to which other realms are attached would then serve as a “super realm” that provides a global view of key statistics across all realms. To configure monitoring access to a realm, log into the realm as a “system administrator” and add users with the role of “observer.” See [“Creating and Editing User Profiles” on page 211](#) for details.

## Configuration Overview

Attach new realms to the current realm (the realm you currently logged into) in Juniper Sky ATP by navigating to **Configure > Global Configuration > Realm Management**. You must enter a Username and Password for the realm in order to attach it.

All the devices and tenant systems on the Enrolled Device page appear in the Realm Management page where you can change their realm associations. See [“Realm Management” on page 124](#) for details.

You should be aware that when you associate realms with devices or change those associations, it changes the way threat management is delivered to those devices, which can affect anti-malware and security-intelligence policies. Be sure all changes in realm/device associations are well-planned and that the consequences are intentional.

Easily alternate between realms using the **Realm** field at the top right of the Web UI. Click inside the realm name field and a drop-down with all available realms appears. Select a new realm to view configurations for that realm. Note that switching between realms is not available for all Web UI pages, only applicable ones.

**NOTE:** You cannot create new security realms from the Realm Management page. To create a security realm, log out of the Web UI. Access the login screen and click the **Create a security realm** link on the bottom left of the login window.

## SRX Series and Tenant System Enrollment

When an SRX Series device is enrolled to Juniper Sky ATP, any tenant systems configured on the device are also enrolled. The names of associated tenant systems appear in the **Host** name field after a colon on the Devices page in Sky ATP. For example, when you run the enroll script on an SRX Series device with the host name **SRX650**, that host name appears in the list of enrolled devices. If SRX650 has several tenant

systems, you would have multiple host name entries starting with SRX650 followed by a colon with the name of the tenant system. For example, **SRX650:subdomain1**.

## RELATED DOCUMENTATION

[Realm Management | 124](#)

[Tenant Systems: Security-Intelligence and Anti-Malware Policies | 126](#)

## Realm Management

Attach new realms to the current realm and change realm associations by navigating to **Configure > Global Configuration > Realm Management**. You must enter a Username and Password for the realm to attach it.

### Note the following:

- Your role must be “system administrator” on Juniper Sky ATP to see the Realm Management page.
- You must explicitly associate an enrolled logical domain with a realm before Juniper Sky ATP can receive submissions from that logical domain.
- Easily switch between realms using the **Realm** field at the top right of the Web UI. Click inside the realm name field and a drop-down with all the realm names appears. Select a new realm to view configurations for that realm. Note that switching between realms is not available for all Web UI pages, only applicable ones. For example, you cannot switch the realm view from the Realm Management page.
- Review the “[Realm Overview](#)” on [page 122](#) topic.
- Have the correct name of the realm you are attaching and your credentials for that realm. You must enter the realm credentials when attaching new realms.
- Realm management makes it easy to change realm/device associations, but when you remove a device’s realm association and create a new one, the new realm begins receiving files and events for that device. The old realm no longer will. Be sure that is your intention before changing existing associations.
- Realm associations are restricted by region. You cannot attach a realm from one region to a realm in another region.

To attach a new realm to the realm you are currently logged into on Juniper Sky ATP, do the following:

1. Navigate to **Configure > Global Configuration > Realm Management**.
2. Click the **Attach Realm** button on the upper right side of the page.

3. In the window, enter the credentials for the realm you are adding. Those are your realm **Username** and realm **Password**. Also enter the **Realm** name.
4. Click **OK**. The realm is added to your list of realms and attached to Juniper Sky ATP.

To associate realms with SRX devices and/or SRX logical domains, do the following:

1. Navigate to **Configure > Global Configuration > Realm Management**.
2. Select a check box beside the realm name and click the **Manage Devices** button on the upper right side of the page. (Note that you can only select one check box at a time for managing devices. If you select more than one check box, the **Manage Devices** button becomes unavailable.)
3. In the window that appears, available devices are listed on the left side. Devices that are already associated with the realm are listed on the right side. Select a device check box, and use the right arrow to associate that device.

To disassociate a device, select the check box in the field on the right and use the left arrow to move that device into the box on the left side.

Changes in associations take place immediately.

**NOTE:** When you remove a device's realm association and create a new one, the new realm begins receiving files and events for that device. The old realm no longer will.

4. Click **OK** to close the window.

To delete one or more attached realms, do the following:

1. Navigate to **Configure > Global Configuration > Realm Management**.
2. Select one or more check boxes beside the realm(s) you want to delete.
3. Click the **X** icon and confirm the delete request.

## RELATED DOCUMENTATION

[Realm Overview](#) | 122

[Tenant Systems: Security-Intelligence and Anti-Malware Policies](#) | 126

## Tenant Systems: Security-Intelligence and Anti-Malware Policies

Tenant systems allow you to allocate virtual system resources, such as memory and CPU, into logical groupings to create multiple virtual firewalls. Each virtual firewall can then identify itself as a stand-alone system within one computing system. Starting in Junos OS 18.4, SRX Series devices support tenant systems for anti-malware and security-intelligence policies. When you associate a tenant system with a realm in Juniper Sky ATP, that tenant system receives the threat management features configured for the realm. The SRX Series device will then perform policy enforcement based on tenant system and the associated Juniper Sky ATP realm.

**NOTE:** For information on using tenant systems with SRX Series devices, please refer to the [Junos documentation](#).

### Tenant System Support for SecIntel Feeds

Starting in Junos OS 18.4, you can configure security-intelligence profiles for tenant systems .

Tenant systems enroll to Sky ATP when the associated SRX Series device is enrolled. All tenant systems with enabled anti-malware or security-intelligence policies appear in the SKY ATP “Enrolled Devices” page with other SRX Series devices.



**WARNING:** Unlike physical devices, which automatically make submissions to the realm they are enrolled in, tenant system submissions are ignored until they are associated with a realm using the Realm Management page in the Juniper Sky ATP Web UI. See [“Realm Management” on page 124](#) for those instructions.

Note that **root-logical-system** is automatically associated with the realm to which the SRX Series device is enrolled. Only **root-logical-system** can make submissions by default. Therefore you do not need to make an association for **root-logical-system**.

Here is an example of the CLI commands for a tenant system security-intelligence policy configuration. The tenant system used in this example (TSYS1) must be associated with the correct realm in Juniper Sky ATP for the policy to get applied to the intended device:

```
set logical-systems TSYS1 services security-intelligence profile pf1 category
Infected-Hosts
set logical-systems TSYS1 services security-intelligence profile pf1 default-rule
then action block drop
```

```

set logical-systems TSYS1 services security-intelligence profile pfl default-rule
then log
set logical-systems TSYS1 services security-intelligence policy p1 Infected-Hosts
pfl

```

Use the following example commands to view the infected hosts feed for a tenant system:

```

root@SRX> show security dynamic-address category-name Infected-Hosts logical-system
TSYS1

```

No.	IP-start	IP-end	Feed	Address
1	10.1.32.131	10.1.32.131	Infected-Hosts/1	ID-2150001a
2	10.1.32.148	10.1.32.148	Infected-Hosts/1	ID-2150001a
3	10.1.32.183	10.1.32.183	Infected-Hosts/1	ID-2150001a
4	10.1.32.201	10.1.32.201	Infected-Hosts/1	ID-2150001a

Or use the following:

```

User1@SRX:TSYS1> show security dynamic-address category-name Infected-Hosts

```

No.	IP-start	IP-end	Feed	Address
1	10.1.32.131	10.1.32.131	Infected-Hosts/1	ID-2150001a
2	10.1.32.148	10.1.32.148	Infected-Hosts/1	ID-2150001a
3	10.1.32.183	10.1.32.183	Infected-Hosts/1	ID-2150001a
4	10.1.32.201	10.1.32.201	Infected-Hosts/1	ID-2150001a

## Tenant System Support for AAMW

Starting in Junos OS 18.4, you can also configure anti-malware policies on a per tenant system basis. Here is an example of a tenant system anti-malware policy configuration:

As stated previously, the tenant system used in this example (TSYS1) must be associated with the correct realm in Sky ATP for the policy to get applied to the intended device. See [“Realm Management” on page 124](#) for Sky ATP Web UI configuration details.

```

set logical-systems TSYS1 services advanced-anti-malware policy LP1 http
inspection-profile ldom_profile
set logical-systems TSYS1 services advanced-anti-malware policy LP1 http action block
set logical-systems TSYS1 services advanced-anti-malware policy LP1 http notification
log
set logical-systems TSYS1 services advanced-anti-malware policy LP1 smtp
inspection-profile default_profile
set logical-systems TSYS1 services advanced-anti-malware policy LP1 smtp notification
log

```

```

set logical-systems TSYS1 services advanced-anti-malware policy LP1 imap
inspection-profile default_profile
set logical-systems TSYS1 services advanced-anti-malware policy LP1 imap notification
log
set logical-systems TSYS1 services advanced-anti-malware policy LP1 verdict-threshold
3

```

Use the following command to view anti-malware policies for a tenant system.

**root@SRX> show services advanced-anti-malware policy logical-systems TSYS1**

```

Advanced-anti-malware configuration:
Policy Name: LP11
Default-notification : Log
Whitelist-notification: Log
Blacklist-notification: Log
Fallback options:
  Action: block
  Notification: No Log
Inspection-profile: ldom_profile
Applications: HTTP
Verdict-threshold: 3
Action: block
Notification: Log

```

Or use the following:

**User1@SRX:TSYS1> show services advanced-anti-malware policy**

```

Advanced-anti-malware configuration:
Policy Name: LP1
Default-notification : Log
Whitelist-notification: Log
Blacklist-notification: Log
Fallback options:
  Action: block
  Notification: No Log
Inspection-profile: ldom_profile
Applications: HTTP
Verdict-threshold: 3
Action: block
Notification: Log

```

## Security Profile CLI

Administrators can configure a single security profile to assign resources to a specific tenant system, use the same security profile for more than one tenant system, or use a mix of both methods. You can configure up to 32 security profiles on an SRX Series device running logical systems.

Security profiles allow you to dedicate various amounts of a resource to the tenant systems and allow them to compete for use of the free resources. They also protect against one logical system exhausting a resource that is required at the same time by other tenant systems.

The following commands are added to the security-profile CLI.

- `aamw-policy`

For example: `set system security-profile <name> aamw-policy maximum 32`

- `secintel-policy`

For example: `set system security-profile <name> secintel-policy maximum 32`

Use the following command to view the security profiles:

`show system security-profile all-resource`

**NOTE:** Refer to the [Junos documentation](#) for more information on the `set system security-profile` command for logical systems.

## RELATED DOCUMENTATION

[Realm Management | 124](#)

[Realm Overview | 122](#)

# 4

PART

## Monitor and Take Action

---

Reports | **131**

Hosts | **137**

Identifying Infected Hosts | **142**

Command and Control Servers | **153**

Identify Hosts Communicating with Command and Control Servers | **158**

File Scanning | **164**

Email Scanning | **173**

Telemetry | **181**

Encrypted Traffic Analysis | **185**

---



# Reports

## IN THIS CHAPTER

- Reports Overview | 131
- Configure Report Definitions | 135

## Reports Overview

You can configure PDF threat assessment reports to be run on-demand or on scheduled intervals. While you cannot determine the information included in the report, you can narrow information to a selected timeframe.

The generated report will contain categories such as the following:

**Table 29: PDF Report Contents**

Report Category	Definition
Executive Summary	<p>An overview report data separated into following categories:</p> <ul style="list-style-type: none"> <li>● Malware—Lists newly discovered malware and known malware.</li> <li>● C&amp;C Server Destinations—Lists C&amp;C server destination.</li> <li>● Infected Hosts—Lists the following:               <ul style="list-style-type: none"> <li>● Infected hosts—Lists the number of potentially infected hosts whose threat level is less than the threshold threat level that is set by the customer.</li> <li>● Blocked hosts—Lists the number of infected hosts that have met the threshold threat level and is blocked by policies configured on the SRX Series device.</li> </ul> </li> <li>● Domains and URLs—Lists the domains and URLs that are suspicious or known to be risky.</li> <li>● High-risk User Data—Lists the following:               <ul style="list-style-type: none"> <li>● Users' computers infected with malware.</li> <li>● High-risk web sites accessed by users.</li> </ul> </li> </ul>

Table 29: PDF Report Contents (continued)

Report Category	Definition
Malware	<p>The malware section contains the following information:</p> <ul style="list-style-type: none"> <li>● Top Malware Identified—Lists the names of the top malware by count.</li> <li>● Top Infected File MIME Types—Lists the top infected multi-purpose Internet mail extensions (MIME) by count.</li> <li>● Top Scanned File Categories—Lists the top file categories that are scanned.</li> </ul>
C&C Server and Malware Locations	<p>This section contains the following information:</p> <ul style="list-style-type: none"> <li>● Top C&amp;C Server Location by Count—Lists the top countries for command and control (C&amp;C) servers by number of communication attempts (C&amp;C hits).</li> <li>● Top Malware Threat Locations by Count—Lists the top countries with malware threats.</li> </ul>
Hosts	<p>This section contains the following information:</p> <ul style="list-style-type: none"> <li>● Top Compromised Hosts—Lists the top hosts that may have been compromised based on their associated threat level.</li> </ul>
Risky Files	<p>This section contains the following information:</p> <ul style="list-style-type: none"> <li>● Top Risky File Categories by Count—Lists the top risky file categories by count for known and newly discovered malicious files.</li> <li>● Top Risky Files Detected by Count—Lists the top risky files detected by count.</li> <li>● Top IPs Detected Attempting to Access Risky Files by Count—Lists the top IP addresses attempting to access risky files.</li> <li>● Top Risky Files Detected by IPs—Lists the top risky files detected per top IP address attempting to access the files.</li> </ul>

Table 29: PDF Report Contents (continued)

Report Category	Definition
Risky Domains, URLs, AND IPs	<p>This section contains the following information: top risky domains, URLs, and IP addresses detected by the number of times access was attempted. It also includes the top users who have attempted to access these risky domains, URLs, and IP addresses.</p> <ul style="list-style-type: none"> <li>● Top Detected Risky Domains, URLs, and IPs by Count—Lists the top risky domains, URLs, and IP addresses detected by the number of times access was attempted.</li> <li>● Most Active Users for Risky Domains, URLs, and IPs by Count—Lists the top users who are most active in attempting to access the risky domains, URLs, and IP addresses by count.</li> <li>● Top Detected Risky Domains, URLs, and IPs by Threat Level—Lists the top risky domains, URLs, and IP addresses detected by the threat level.</li> </ul>

Table 29: PDF Report Contents (continued)

Report Category	Definition
Email	<p>This section contains the list of actions taken on scanned emails. It also includes email attachments determined to be malware and users who are risky email senders.</p> <ul style="list-style-type: none"> <li>● Actions Taken—Lists the action taken for scanned e-mail.</li> <li>● High-Risk Email Data—Lists the count of e-mail attachments with malware and risky senders.</li> <li>● Malicious SMTP Email by Count—The report breaks scanned e-mail down by protocol and lists SMTP e-mails found to be malicious.</li> <li>● Malicious IMAP Email by Count—The report breaks scanned e-mail down by protocol and lists IMAP e-mails found to be malicious.</li> <li>● Top Risky File Categories Detected for Email Attachments—Lists the top risky file categories that were detected from files received as e-mail attachments.</li> <li>● Top Risky Email Attachments Detected by Count—Lists the top risky files that are detected from email attachments.</li> <li>● Top Users Receiving Risky Email Attachments—Lists the top users who are receiving risky file attachments through e-mail.</li> <li>● Top Risky Email Attachments Detected per Top Users—Lists the top users and their most risky file attachments.</li> <li>● Top Risky Email Sender Domains by Count—Lists the top risky sender domains based on the threat level of file attachments sent in email.</li> <li>● Top Sender Domains of Risky File Attachments by Count—Lists the top sender domains with risky file attachments and the count of how many times the the risky file attachments that were detected.</li> <li>● Actions on SMTP Malicious Email by Count—Lists actions taken for malicious SMTP e-mails.</li> <li>● Actions on IMAP Malicious Email by Count—Lists actions taken for malicious IMAP e-mails.</li> </ul>

## RELATED DOCUMENTATION

| [Configure Report Definitions](#) | 135

## Configure Report Definitions

Use the available fields to build a report that runs at set intervals and automatically sends the PDF report to the email addresses you specify.

In addition to creating your own report definition, you can use the included, pre-defined, read-only, on-demand reports. The included reports are named as follows:

- Threat Assessment Last Day
- Threat Assessment Last Week
- Threat Assessment Last Month

To run a pre-defined, read-only, on-demand report, select the check box for the report in the list view and click the **Run Now** button at the top of the list view page

**NOTE:** Once a report is run, it is listed in the **Reports>Generated Reports** page for viewing anytime.

Do the following to configure a custom report definition:

1. Navigate to **Reports>Report Definitions**.
2. Click the + (Create) icon on the top right of the page. The Report Definition window appears.
3. Enter the following information into the Report Definition window.

**Table 30: Report Definition Fields**

Field	Description
Name	Enter a name for the report. This is a unique string that must begin with an alphanumeric character and can include dashes, spaces, and underscores; 63-character maximum.
Description	Give the report a detailed description that all administrators can recognize.
Date Range Options	Configure a recurring schedule for running a report. The options are: Last Day (daily), Last Week (once weekly), and Last Month (once monthly). Based on your selection, you will configure more a specific time period in the next field.

Table 30: Report Definition Fields (continued)

Field	Description
Generate Report Every	<p>Use the downward arrow in the entry field for adding multiple days. Use the X to remove a day.</p> <p>If you selected Last Day in the previous field, choose multiple days of the week for running a report. For example, every day (add all days manually Sunday through Saturday) or only add Monday, Wednesday, and Friday for an every other day report.</p> <p>If you selected Last Week, choose one day of the week for running a weekly report.</p> <p>If you selected Last Month, choose whether to run a report on the first day of the month or the last day of the month.</p>
Email Recipients	<p>Once a report is generated, you can have it sent to one or more email addresses. The email addresses available for receiving reports come from the <b>Administrator &gt; Users</b> list.</p> <p>Note that once the report is created, you can always send it to an email address on-demand by selecting the check box for the report in the list view and clicking the Send button at the top of the page. A new window appears, and you can select an email address there. Again, the available addresses come from the <b>Administrator &gt; Users</b> list.</p>

Once a report is generated, it is listed as a downloadable PDF file in the **Reports>Generated Reports** page for viewing anytime.

4. Click **OK** to save the report definition.

#### RELATED DOCUMENTATION

| [Reports Overview](#) | 131

# Hosts

## IN THIS CHAPTER

- Hosts Overview | 137
- Host Details | 140

## Hosts Overview

Access this page from the **Monitor** menu.

The hosts page lists compromised hosts and their associated threat levels. From here, you can monitor and mitigate malware detections on a per host basis.

**NOTE:** User notification of infected hosts—As of Junos OS 18.1R1, there is support HTTP URL redirection based on infected hosts with the block action. This is configured through the CLI on the SRX Series device using the **set services security-intelligence profile** command. See the [Juniper Sky ATP CLI Reference Guide](#) for details.

Compromised hosts are systems for which there is a high confidence that attackers have gained unauthorized access. When a host is compromised, the attacker can do several things to the computer, such as:

- Send junk or spam e-mail to attack other systems or distribute illegal software.
- Collect personal information, such as passwords and account numbers.

Compromised hosts are listed as secure intelligence data feeds (also called information sources.) The data feed lists the IP address of the host along with a threat level; for example, 130.131.132.133 and threat level 5. Once threats are identified, you can create threat prevention policies to take enforcement actions on the inbound and outbound traffic on these infected hosts. See “[Global Configuration for Infected Hosts](#)” on page 116 for more information.

For the Hosts listed on this page, you can perform the following actions on one or multiple hosts at once:

Table 31: Operations for Multiple Infected Hosts

Action	Definition
Export Data	Click the Export button to download compromised host data to a CSV file. You are prompted to narrow the data download to a selected time-frame.
Set Policy Override	<p>Select the check box beside one or multiple hosts and choose one of the following options: Use configured policy (not included in infected hosts feed), Always include host in infected hosts feed, Never include host in infected hosts feed.</p> <p><b>NOTE:</b> The policy referred to here is the policy configured on the SRX Series device. See <a href="#">“Example: Configuring a Juniper Sky Advanced Threat Prevention Policy Using the CLI”</a> on page 197.</p>
Set Investigation Status	Select the check box beside one or multiple hosts and choose one of the following options: Resolved - false positive, Resolved - fixed, and Resolved - ignored.

**NOTE:** When you select a **Policy Override** option for hosts, other dependent status fields, such as Infected Host Feed, will also change accordingly. In some cases, you may have to refresh the page to see the updated information.

The following information is available in the Host table.

Table 32: Compromised Host Information

Field	Description
Host Identifier	<p>The Juniper Sky ATP-assigned name for the host. This name is created by Juniper Sky ATP using known host information such as IP address, MAC address, user name, and host name. The assigned name will be in the following format: <b>username@server</b>. If the username is not known and MAC address or IP address are used, the name may appear as any of the following formats:</p> <p><b>user01@aa:bb:cc:dd:ee:ff, user02@1.1.1.1 or 1.1.1.1</b></p> <p><b>NOTE:</b> You can edit this name. If you edit the Juniper Sky ATP-assigned name, Juniper Sky ATP will recognize the new name and not override it.</p>
Host IP	The IP address of the compromised host.



Table 32: Compromised Host Information (*continued*)

Field	Description
Threat Level	<p>A number between 0 -10 indicating the severity of the detected threat, with 10 being the highest.</p> <p><b>NOTE:</b> Click the three vertical dots at the top of the column to filter the information on the page by threat level.</p>
Infected Host Feed	<p>Displays the current host feed settings:</p> <ul style="list-style-type: none"> <li>• <b>Included:</b> This is the default policy. The host is included in the infected host feed if its threat level meets the set infected host threshold.</li> <li>• <b>Excluded:</b> The host is whitelisted and will be excluded from the infected host feed even if its threat level meets the threshold.</li> <li>• <b>Included Manually:</b> The host is blacklisted and will be included in infected host feed even if its threat level does not meet the threshold.</li> </ul>
Threat First Seen	The date and time the threat was seen for the first time.
Threat Last Seen	The date and time of the most recent detection of the threat.
C&C Hits	<p>The number of times a command and control server communication threat with this host was detected.</p> <p><b>NOTE:</b> Click the three vertical dots at the top of the column to filter the information on the page by C&amp;C hits.</p>
Malware	<p>The number of times a malware threat was downloaded by this host.</p> <p><b>NOTE:</b> Click the three vertical dots at the top of the column to filter the information on the page by malware detections.</p>
State of Investigation	Displays either Open, In progress, Resolved-False positive, Resolved-Fixed, Resolved-Ignored

## RELATED DOCUMENTATION

[Host Details | 140](#)

[Global Configuration for Infected Hosts | 116](#)

[HTTP File Download Overview | 164](#)

[HTTP File Download Details | 166](#)

[Manual Scanning Overview | 169](#)

## Host Details

Access this page by clicking the Host Identifier from the **Monitor >Hosts** page. Double click on the host to view summary details and malicious files that have been downloaded.

Use the host details page to view in-depth information about current threats to a specific host by time frame. From here you can change the host identifier, the investigation status, and the blocked status of the host.

The information provided on the host details page is as follows:

**Table 33: Threat Level Recommendations**

Threat Level	Definition
0	Clean; no action is required.
1-3	Low threat level. Recommendation: Disable this host.
4-6	Medium threat level. Recommendation: Disable this host.
7-10	High threat level. Host has been automatically blocked.

- **Host Identifier**—Displays the Juniper Sky ATP-assigned name of the host. You can edit this name by entering a new name in this field and clicking **Save**. To return to the default assigned name, click **Reset**.
- **Host IP Address**—Displays the IP address of the selected host.
- **MAC Address**—This information is only available when Juniper Sky ATP is used with Policy Enforcer.
- **Host Status**—Displays the current threat level of the host and recommended actions.
- **Investigation Status**—The following states of investigation are available: Open, In progress, Resolved - false positive, Resolved - fixed, and Resolved - ignored.
- **Policy override for this host**—The following options are available: Use configured policy (not included in infected hosts feed), Always include host in infected hosts feed, Never include host in infected hosts feed.

**NOTE:** The blocked status changes in relation to the investigation state. For example, when a host changes from an open status (Open or In Progress) to one of the resolved statuses, the blocked status is changed to allowed and the threat level is brought down to 0. Also, when the investigation status is changed to resolved, an event is added to the log at the bottom of the page.

- Host threat level graph—This is a color-coded graphical representation of threats to this host displayed by time frame. You can change the time frame, and you can slide the graph backward or forward to zoom in or out on certain times. When you zoom in, you can view individual days within a month.
- Expand time-frame to separate events—Use this check box to stretch a period of time and see the events spread out individually.
- Past threats—The date and status of past threats to this host are listed here. The time frame set previously also applies to this list. The description for each event provides details about the threat and the action taken at the time.

#### RELATED DOCUMENTATION

---

[Hosts Overview | 137](#)

---

[HTTP File Download Overview | 164](#)

---

[HTTP File Download Details | 166](#)

---

[Manual Scanning Overview | 169](#)

# Identifying Infected Hosts

## IN THIS CHAPTER

- [Compromised Hosts: More Information | 142](#)
- [Configuring the SRX Series Devices to Block Infected Hosts | 149](#)

## Compromised Hosts: More Information

Infected hosts are systems where there is a high confidence that attackers have gained unauthorized access. When a host is compromised, the attacker can do several things to the computer, such as:

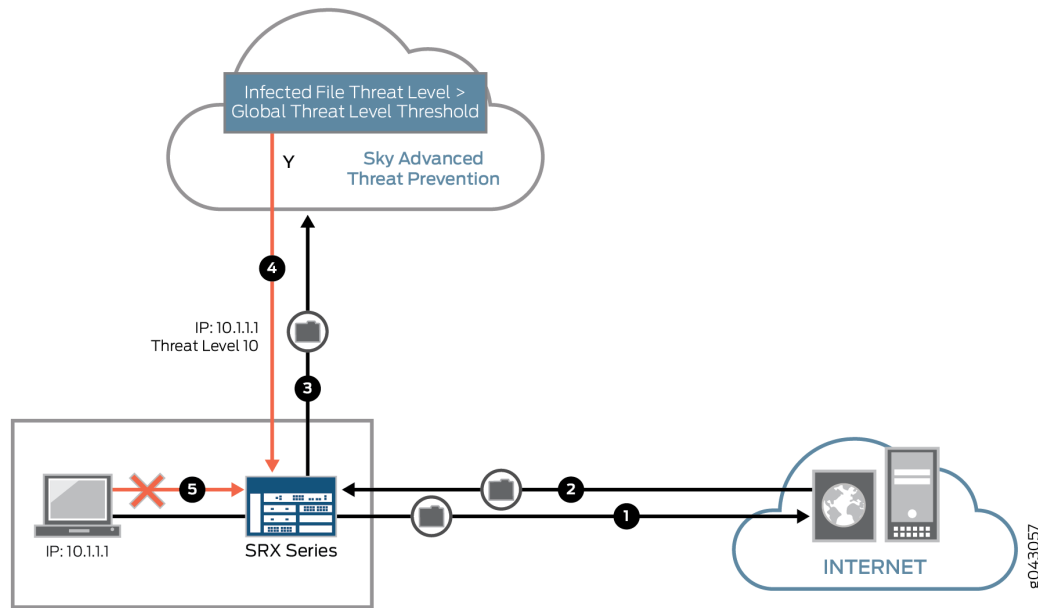
- Send junk or spam e-mail to attack other systems or distribute illegal software.
- Collect personal information, such as passwords and account numbers.
- Disable your computer's security settings to allow easy access.

Infected hosts are listed as IP address or IP subnet of the host along with a threat level, for example, xxx.xxx.xxx.133 and threat level 5. Once identified, Juniper Sky ATP recommends an action and you can create security policies to take enforcement actions on the inbound and outbound traffic on these infected hosts. Juniper Sky ATP uses multiple indicators, such as a client attempting to contact a C&C server or a client attempting to download malware, and a proprietary algorithm to determine the infected host threat level.

The data feed URL is set up automatically for you when you run the `op` script to configure your SRX Series device. See [“Downloading and Running the Juniper Sky Advanced Threat Prevention Script” on page 24](#).

[Figure 20 on page 143](#) shows one example of how devices are labelled as infected hosts by downloading malware.

Figure 20: Infected Host from Malware



Step	Description
1	A client with IP address 10.1.1.1 is located behind an SRX Series device and requests a file to be downloaded from the Internet.
2	The SRX Series device receives the file from the Internet and checks its security policies to see if any action needs to be taken before sending the file to the client.
3	The SRX Series device has a Juniper Sky ATP policy that requires files of the same type that was just downloaded to be sent to the cloud for inspection.  This file is not cached in the cloud, meaning this is the first time this specific file has been sent to the cloud for inspection, so the SRX Series device sends the file to the client while the cloud performs an exhaustive inspection.
4	In this example, the cloud analysis determines the file has a threat level greater than the threshold indicating that the file is malware, and sends this information back to the SRX Series device.  The client is placed on the infected host list.
5	Juniper Sky ATP blocks the client from accessing the Internet.  The client remains on the infected host list until an administrator performs further analysis and determines it is safe.

You can view the status of hosts from the Juniper Sky ATP Web Portal by navigating to **Monitor > Hosts**. You can also use the **show services security-intelligence statistics** CLI command on the SRX Series device to view a quick report.

```
host> show services security-intelligence statistics
Category Infected-Hosts:
  Profile pr2:
    Total processed sessions: 37
    Permit sessions:          0
    Block drop sessions:     35
    Block close sessions:    2
```

An email can be configured in the **Configure > Global Configuration > Infected Hosts** window to alert users when a host's threat level is at or above a specified threshold.

A malware and host status event syslog message is created in `/var/log/messages`. Junos OS supports forwarding logs using stream mode and event mode. For information on JSA and QRadar SIEM support, see [Juniper Sky ATP Supported Platforms Guide](#).

**NOTE:** To use syslog, you must configure system logging for all SRX Series device within the same realm. For example, if REALM1 contains SRX1 and SRX2, both SRX1 and SRX2 must have system logging enabled. For more information on configuring system logging, see [SRX Getting Started - System Logging](#).

- Malware event syslog using stream mode.

```
Sep 20 00:01:14 6.0.0.254 host-example RT_AAMW: AAMW_MALWARE_EVENT_LOG:
timestamp=Thu Jun 23 09:55:38 2016 tenant-id=ABC123456 sample-sha256=ABC123
client-ip=192.0.2.0 mw-score=9 mw-info=Eicar:TestVirus client-username=admin
client-hostname=host.example.com
```

- Host status event syslog using stream mode.

```
Sep 20 00:01:54 6.0.0.254 host-example RT_AAMW: AAMW_HOST_INFECTED_EVENT_LOG:
timestamp=Thu Jun 23 09:55:38 2016 tenant-id=ABC123 client-ip=192.0.2.0
client-hostname=host.example.com host-status=in_progress host-policy=default
threat-level=7 infected-host-status=added reason=malware details=malware analysis
detected host downloaded a malicious_file with score 9, sha256 ABC123
```

- Malware event syslog using event mode.

```
<14>1 2016-09-20T10:43:30.330-07:00 host-example RT_AAMW - AAMW_MALWARE_EVENT_LOG
[junos@xxxx.1.1.x.x.xxx timestamp="Thu Jun 23 09:55:38 2016" tenant-id="ABC123456"
sample-sha256="ABC123" client-ip-str="192.0.2.0" verdict-number="9"
malware-info="Eicar:TestVirus" username="admin" hostname="host.example.com"]
timestamp=Thu Jun 23 09:55:38 2016 tenant-id=ABC123456 sample-sha256=ABC123
client-ip=172.24.0.12 mw-score=9 mw-info=Eicar:TestVirus client-username=admin
client-hostname=host.example.com
```

- Host status event syslog using event mode.

```
<11>1 2016-09-20T10:40:30.050-07:00 host-example RT_AAMW -
AAMW_HOST_INFECTED_EVENT_LOG [junos@xxxx.1.1.x.x.xxx timestamp="Thu Jun 23 09:55:38
2016" tenant-id="ABC123456" client-ip-str="192.0.2.0" hostname="host.example.com"
status="in_progress" policy-name="default" th="7" state="added" reason="malware"
message="malware analysis detected host downloaded a malicious_file with score
9, sha256 ABC123"] timestamp=Thu Jun 23 09:55:38 2016 tenant-id=ABC123456
client-ip=192.0.2.0 client-hostname=host.example.com host-status=in_progress
host-policy=default threat-level=7 infected-host-status=added reason=malware
details=malware analysis detected host downloaded a malicious_file with score 9,
sha256 ABC123
```

The syslog record contains the following fields:

Field	Description
timestamp	Date and time the syslog entry is created.
tenant_id	Internal unique identifier.
sample_sha256	SHA-256 hash value of the downloaded file.
client_ip	Client IP address, supporting both IP4 and IP6.
mw_score	Malware score. This is an integer between 0-10.
mw_info	Malware name or brief description.
client_username	Username of person that downloaded the possible malware.
client_hostname	Hostname of device that downloaded the possible malware.
host_status	Host status. Currently it is only <b>in_progress</b> .

Field	Description
host_policy	Name of Juniper Sky ATP policy that enforced this action.
threat_level	Host threat level. This is an integer between 0-10.
infected_host_status	Infected host status. It can be one of the following: <b>Added, Cleared, Present, Absent.</b>
reason	Reason for the log entry. It can be one of the following: <b>Malware, CC, Manual.</b>
details	Brief description of the entry reason, for example: <b>malware analysis detected host downloaded a malicious_file with score 9, sha256 abc123</b>

## About Block Drop and Block Close

If you use the **show services security-intelligence statistics** CLI command, you'll see block drop and block close sessions.

```
host> show services security-intelligence statistics
Category Infected-Hosts:
  Profile pr2:
    Total processed sessions: 37
    Permit sessions:          0
    Block drop sessions:      35
    Block close sessions:     2
```

You can configure either block drop or block close. If you choose block drop, then the SRX Series device silently drops the session's packet and the session eventually times out. If block close is configured, the SRX Series devices sends a TCP RST packet to the client and server and the session is dropped immediately.

You can use block close, for example, to protect the resource of your client or server. It releases the client and server sockets immediately. If client or server resources is not a concern or you don't want anyone to know there is a firewall located in the network, you can use block drop.

Block close is valid only for TCP traffic. Non-TCP traffic uses block drop even if you configure it block close. For example, if you configure infected hosts to block close:

```
...
set services security-intelligence profile pr2 rule r2 then action block close
...
```

when you send icmp traffic through the device, it is block dropped.



For more information on setting block drop and block close, see [“Configuring the SRX Series Devices to Block Infected Hosts”](#) on page 149.

## Host Details

Click the host IP address on the hosts main page to view detailed information about current threats to the selected host by time frame. From the details page, you can also change the investigation status and the blocked status of the host. For more information on the host details, see the web UI tooltips and online help.

You can also use the **show security dynamic-address category-name Infected-Hosts** CLI command to view the infected host list.

```
host> show security dynamic-address category-name Infected-Hosts
No.      IP-start      IP-end        Feed          Address
1        x.0.0.7       x.0.0.7       Infected-Hosts/1 ID-21500011
2        x.0.0.10      x.0.0.10      Infected-Hosts/1 ID-21500011
3        x.0.0.21      x.0.0.21      Infected-Hosts/1 ID-21500011
4        x.0.0.11      x.0.0.11      Infected-Hosts/1 ID-21500012
5        x.0.0.12      x.0.0.12      Infected-Hosts/1 ID-21500012
6        x.0.0.22      x.0.0.22      Infected-Hosts/1 ID-21500012
7        x.0.0.6       x.0.0.6       Infected-Hosts/1 ID-21500013
8        x.0.0.9       x.0.0.9       Infected-Hosts/1 ID-21500013
9        x.0.0.13      x.0.0.13      Infected-Hosts/1 ID-21500013
10       x.0.0.23      x.0.0.23      Infected-Hosts/1 ID-21500013
11       x.0.0.14      x.0.0.14      Infected-Hosts/1 ID-21500014
12       x.0.0.24      x.0.0.24      Infected-Hosts/1 ID-21500014
13       x.0.0.1       x.0.0.1       Infected-Hosts/1 ID-21500015
14       x.0.0.2       x.0.0.2       Infected-Hosts/1 ID-21500015
15       x.0.0.3       x.0.0.3       Infected-Hosts/1 ID-21500015
16       x.0.0.4       x.0.0.4       Infected-Hosts/1 ID-21500015
17       x.0.0.5       x.0.0.5       Infected-Hosts/1 ID-21500015
18       x.0.0.15      x.0.0.15      Infected-Hosts/1 ID-21500015
19       x.0.0.25      x.0.0.25      Infected-Hosts/1 ID-21500015
20       x.0.0.16      x.0.0.16      Infected-Hosts/1 ID-21500016
21       x.0.0.26      x.0.0.26      Infected-Hosts/1 ID-21500016
22       x.0.0.17      x.0.0.17      Infected-Hosts/1 ID-21500017
23       x.0.0.27      x.0.0.27      Infected-Hosts/1 ID-21500017
24       x.0.0.18      x.0.0.18      Infected-Hosts/1 ID-21500018
25       x.0.0.28      x.0.0.28      Infected-Hosts/1 ID-21500018
26       x.0.0.19      x.0.0.19      Infected-Hosts/1 ID-21500019
27       x.0.0.29      x.0.0.29      Infected-Hosts/1 ID-21500019
28       x.0.0.8       x.0.0.8       Infected-Hosts/1 ID-2150001a
29       x.0.0.20      x.0.0.20      Infected-Hosts/1 ID-2150001a
```

```
30      x.0.0.30      x.0.0.30      Infected-Hosts/1 ID-2150001a
```

```
Total number of matching entries: 30
```

### **Automatic Lowering of Host Threat Level or Removal from Infected Hosts Feed**

The threat level of a host may decrease automatically if there have been no security events for that host for the period of one month. The month in question is a rolling window of time relative to the current time. The number and type of events seen over that month determine the threat level score of the host. A host may automatically be removed from the infected hosts list by the same process, if all malware events fall outside of that month long window.

If the manual resolution of a host takes place and the threat level is set to zero, but another malware event occurs, the resolution event is ignored and the resulting threat score for the host once again takes into consideration all the suspicious events within the period of one month to determine the new threat score.

## Configuring the SRX Series Devices to Block Infected Hosts

An Infected-Host feed lists the hosts that have been compromised and need to be quarantined from communicating with other devices. The feed is in the format of IP addresses all with a threat level of 10, for example xxx.xxx.xxx.133 with threat level 10. You can configure security policies to take enforcement actions on the inbound and outbound traffic to and from a host whose IP address is listed in the feed. The Infected-Host feed is downloaded to the SRX Series device only when the infected host profile is configured and enabled in a firewall policy.

**NOTE:** Once the Juniper Sky ATP global threshold for is met for an infected host (see [“Global Configuration for Infected Hosts” on page 116](#)), that host is added to the infected hosts feed and assigned a threat level of 10 by the cloud. Therefore all IP addresses in the infected hosts feed are threat level 10.

To create the infected host profile and policy and firewall policy:

1. Define a profile for both the infected host and CC. In this example, the infected host profile is named **ih-profile** and the action is block drop anything with a threat level higher than 5. The CC host profile is named **cc-profile** and is based on outbound requests to a C&C host, so add C&C rules to the profile (threat levels 8 and above are blocked.)

```

root@host#
set services security-intelligence profile ih-profile category Infected-Hosts
rule if-rule match threat-level [5 6 7 8 9 10]
root@host# set services security-intelligence profile ih-profile category
Infected-Hosts rule if-rule then action block drop
root@host# set services security-intelligence profile ih-profile category
Infected-Hosts rule if-rule then log

root@host# set services security-intelligence profile cc-profile category CC
root@host# set services security-intelligence profile cc-profile rule CC_rule
match threat-level [8 9 10]
root@host# set services security-intelligence profile cc-profile rule CC_rule
then action block drop
root@host# set services security-intelligence profile cc-profile rule CC_rule
then log
root@host# set services security-intelligence profile cc-profile default-rule
then action permit

```

As of Junos 18.1R1, there is support for the block action with HTTP URL redirection for Infected Hosts. During the processing of a session IP address, if the IP address is on the infected hosts list and HTTP traffic is using ports 80 or 8080, infected hosts HTTP redirection can be done. If HTTP traffic is using dynamic ports, HTTP traffic redirection cannot be done. See command below.

2. Verify your command using the **show services security-intelligence** CLI command. It should look similar to this:

```

root@host# show services security-intelligence profile ih-profile
category Infected-Hosts;
rule if-rule {
  match {
    threat-level [ 5 6 7 8 9 10 ];
  }
  then {
    action {
      block {
        drop;
      }
    }
  }
}

```

```

        log;
    }
}

```

```

root@host# show services security-intelligence profile cc-profile
category CC;
rule CC_rule {
    match {
        threat-level [ 8 9 10 ];
    }
    then {
        action {
            block {
                drop;
            }
        }
        log;
    }
}

```

3. Configure the security intelligence policy to include both profiles created in Step 1. In this example, the policy is named **infected-host-cc-policy**.

```

root@host# set services security-intelligence policy infected-host-cc-policy
Infected-Hosts ih-profile
root@host# set services security-intelligence policy infected-host-cc-policy CC
cc-profile

```

4. Configure the firewall policy to include the security intelligence policy. This example sets the trust-to-untrust zone.

```

root@host# set security policies from-zone trust to-zone untrust policy p2 match
source-address any destination-address any application any
root@host# set security policies from-zone trust to-zone untrust policy p2 then
permit application-services security-intelligence-policy infected-host-cc-policy

```

5. Verify your command using the **show security policies** CLI command. It should look similar to this:

```

root@host# show security policies
...

```

```
from-zone trust to-zone untrust {  
  policy p2 {  
    match {  
      source-address any;  
      destination-address any;  
      application any;  
    }  
    then {  
      permit {  
        application-services {  
          security-intelligence-policy infected-host-cc-policy;  
        }  
      }  
    }  
  }  
}  
...  
[edit]
```

6. Commit your changes.

# Command and Control Servers

## IN THIS CHAPTER

- [Command and Control Servers Overview | 153](#)
- [Command and Control Server Details | 154](#)

## Command and Control Servers Overview

Access this page from the **Monitor** menu.

**NOTE:** C&C and Geo IP filtering feeds are only available with a Juniper Sky ATP premium or basic license.

**NOTE:** At this time, C&C URL feeds are not supported with SSL forward proxy.

The C&C servers page lists information on servers that have attempted to contact and compromise hosts on your network. A C&C server is a centralized computer that issues commands to botnets (compromised networks of computers) and receives reports back from them.

### Benefits of Command and Control Server Feeds

- Using C&C feeds adds another layer of protection to your network, preventing the creation of botnets from within your network. Botnets gather sensitive information, such as account numbers or credit card information, and participate in distributed denial-of-service (DDoS) attacks.
- Using C&C feeds also prevents botnets from communicating with hosts within your network in an attempt to gather information or launch an attack.

**NOTE:** You can whitelist C&C servers from the details page. See [“Command and Control Server Details” on page 154](#).

The following information is available on this page.

**Table 34: Command & Control Server Data Fields**

Field	Definition
C&C Server	The IP address of the suspected command and control server.
C&C Threat Level	The threat level of the C&C server as determined by an analysis of actions and behaviors.
Hits	The number of times the C&C server has attempted to contact hosts on your network.
C&C Country	The country where the C&C server is located.
Last Seen	The date and time of the most recent C&C server hit.
Protocol	The protocol (TCP or UDP) the C&C server used to attempt communication.
Client Host	The IP address of the host the C&C server attempted to communicate with.
Action	The action taken on the communication (permitted or blocked).

## RELATED DOCUMENTATION

[Command and Control Server Details | 154](#)

[Host Details | 140](#)

[Hosts Overview | 137](#)

## Command and Control Server Details

Access this page by clicking on an **External Server IP** link from the **Command and Control Servers** page.

Use Command and Control Server Details page to view analysis information and a threat summary for the C&C server. The following information is displayed for each server.

- Total Hits
- Threat Summary (Threat level, Location, Category, Time last seen)
- Ports and protocols used



This page is divided into several sections:

**Table 35: Options on the C&C Server Details Page (Upper Right Side of Page)**

Button/Link	Purpose
Select Option > Add to Whitelist	<p>Choose this option to add the C&amp;C server to the whitelist.</p> <p><b>WARNING:</b> Adding a C&amp;C server to the whitelist automatically triggers a remediation process to update any affected hosts (in that realm) that have contacted the newly whitelisted C&amp;C server.</p> <p>All C&amp;C events related to this whitelisted server will be removed from the affected hosts' events, and a host threat level recalculation will occur.</p> <p>If the host score changes during this recalculation, a new host event appears describing why it was rescored. (For example, "Host threat level updated after C&amp;C server 1.2.3.4 was cleared.") Additionally, the server will no longer appear in the list of C&amp;C servers because it has been cleared.</p> <p><b>NOTE:</b> You can also whitelist C&amp;C servers from the <b>Configuration &gt; Whitelist</b> page. See "<a href="#">Creating Whitelists and Blacklists</a>" on page 59 for details.</p>
Select Option > Report False Positive	<p>Choose this option to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report, however, this does not change the verdict.</p>

Under Time Range is a graph displaying the frequency of events over time. An event occurs when a host communicates to the C&C server IP address (either sending or receiving data). You can filter this information by clicking on the time-frame links: 1 day, 1 week, 1 month, Custom (select your own time-frame).

**Hosts** is a list of hosts that have contacted the server. The information provided in this section is as follows:

**Table 36: Command & Control Server Contacted Host Data**

Field	Definition
Client Host	The name of the host in contact with the command and control server.
Client IP Address	The IP address of the host in contact with the command and control server. (Click through to the Host Details page for this host IP.)
C&C Threat Level	The threat level of the C&C server as determined by an analysis of actions and behaviors at the time of the event.
Action	The action taken by the device on the communication (whether it was permitted or blocked).

Table 36: Command &amp; Control Server Contacted Host Data (continued)

Field	Definition
Protocol	The protocol (TCP or UDP) the C&C server used to attempt communication.
Port	The port the C&C server used to attempt communication.
Device Name	The name of the device in contact with the command and control server.
Date Seen	The date and time of the most recent C&C server hit.
Username	The name of the host user in contact with the command and control server.

**Domains** is a list of domains that the IP address has previously used at the time of suspicious events. If a C&C IP address is seen changing its DNS/domain name to evade detection, a list of the various names used will be listed along with the dates in which they were seen.

Table 37: Command &amp; Control Server Associated Domains Data

Field	Definition
Client Host	This is a list of domains the destination IP addresses in the C&C server events resolved to.
Last Seen	The date and time of the most recent C&C server hit.

**Signatures** is a list of the threat indicators associated with the IP address. The C&C server blocked by the Juniper “Global Threat Feed” will show domains and/or signatures. (The “Blocked Via” column, under the C&C servers listing, shows whether a C&C server IP address was found in the Juniper “Global Threat Feed” or in a different configured custom feed.)

Table 38: Command &amp; Control Server Signature Data

Field	Definition
Name	The name or type of detected malware.
Category	Description of the malware and way in which it may have compromised a resource or resources.
Date	The date the malware was seen.

## RELATED DOCUMENTATION

[Command and Control Servers Overview | 153](#)

---

[Host Details | 140](#)

---

[Hosts Overview | 137](#)

# Identify Hosts Communicating with Command and Control Servers

## IN THIS CHAPTER

- [Command and Control Servers: More Information | 158](#)
- [Configuring the SRX Series Device to Block Outbound Requests to a C&C Host | 161](#)

## Command and Control Servers: More Information

Command and control (C&C) servers remotely send malicious commands to a botnet, or a network of compromised computers. The botnets can be used to gather sensitive information, such as account numbers or credit card information, or to participate in a distributed denial-of-service (DDoS) attack.

When a host on your network tries to initiate contact with a possible C&C server on the Internet, the SRX Series device can intercept the traffic and perform an enforcement action based on real-time feed information from Juniper Sky ATP. The Web UI identifies the C&C server IP address, its threat level, number of times the C&C server has been contacted, etc.

An **FP/FPN** button lets you report false positive or false negative for each C&C server listed. When reporting false negative, Juniper Sky ATP will assign a C&C threat level equal to the global threat level threshold you assign in the global configuration (**Configure > Global Configuration**).

Juniper Sky ATP blocks that host from communicating with the C&C server and can allow the host to communicate with other servers that are not on the C&C list depending on your configuration settings. The C&C threat level is calculated using a proprietary algorithm.

You can also use the **show services security-intelligence statistics** or **show services security-intelligence statistics profile *profile-name*** CLI commands to view C&C statistics.

```
user@root> show services security-intelligence statistics
Category Whitelist:
  Profile Whitelist:
    Total processed sessions: 0
    Permit sessions:          0
```

```

Category Blacklist:
  Profile Blacklist:
    Total processed sessions: 0
    Block drop sessions:      0
Category CC:
  Profile cc_profile:
    Total processed sessions: 5
    Permit sessions:         4
    Block drop sessions:     1
    Block close sessions:    0
    Close redirect sessions: 0
Category JWAS:
  Profile Sample-JWAS:
    Total processed sessions: 0
    Permit sessions:         0
    Block drop sessions:     0
    Block close sessions:    0
    Close redirect sessions: 0
Category Infected-Hosts:
  Profile hostintel:
    Total processed sessions: 0
    Permit sessions:         0
    Block drop sessions:     0
    Block close sessions:    0

```

In the following example, the C&C profile name is **cc\_profile**.

```

user@root> show services security-intelligence statistics profile cc_profile
Category CC:
  Profile cc_profile:
    Total processed sessions: 5
    Permit sessions:         4
    Block drop sessions:     1
    Block close sessions:    0
    Close redirect sessions: 0

```

You can also use the **show services security-intelligence category detail category-name *category-name* feed-name *feed-name* count *number* start *number*** CLI command to view more information about the C&C servers and their threat level.

**NOTE:** Set both count and start to 0 to display all C&C servers.

For example:

```
user@root> show services security-intelligence category detail category-name CC
feed-name cc_url_data count 0 start 0
Category name      :CC
  Feed name        :cc_url_data
  Version          :20160419.2
  Objects number   :24331
  Create time      :2016-04-18 20:43:59 PDT
  Update time      :2016-05-04 11:39:21 PDT
  Update status    :Store succeeded
  Expired          :No
  Options          :N/A
  { url:http://g.xxxxx.net threat_level:9}
  { url:http://xxxx.xxxxx.net threat_level:9}
  { url:http://xxxxx.pw threat_level:2}
  { url:http://xxxxx.net threat_level:9}
  ...
```

## RELATED DOCUMENTATION

| [Configuring the SRX Series Device to Block Outbound Requests to a C&C Host](#) | 161

## Configuring the SRX Series Device to Block Outbound Requests to a C&C Host

The C&C feed lists devices that attempt to contact a C&C host. If an outbound request to a C&C host is attempted, the request is blocked and logged or just logged, depending on the configuration. Currently, you configure C&C through CLI commands and not through the Web interface.

To create the C&C profile and policy and firewall policy:

1. Configure the C&C profile. In this example the profile name is **cc\_profile** and threat levels 8 and above are blocked.

```
root@host# set services security-intelligence profile cc_profile category CC
root@host# set services security-intelligence profile cc_profile rule CC_rule
match threat-level [8
9 10]
root@host# set services security-intelligence profile cc_profile rule CC_rule
then action block drop
root@host# set services security-intelligence profile cc_profile rule CC_rule
then log
root@host# set services security-intelligence profile cc_profile default-rule
then action permit
```

2. Verify your profile is correct using the **show services security-intelligence** CLI command. Your output should look similar to this.

```
root@host# show services security-intelligence profile cc_profile
category CC;
rule CC_rule {
    match {
        threat-level [ 8 9 10 ];
    }
    then {
        action {
            block {
                drop;
            }
        }
        log;
    }
}
default-rule {
```

```

    then {
        action {
            permit;
        }
        log;
    }
}

```

3. Configure your C&C policy to point to the profile created in Step 1. In this example, the C&C policy name is **cc\_policy**.

```

root@host# set services security-intelligence policy cc_policy CC cc_profile

```

4. Verify your policy is correct using the **show services security-intelligence** CLI command. Your output should look similar to this.

```

root@host# show services security-intelligence policy cc_policy
CC {
    cc_profile;
}

[edit]

```

5. Configure the firewall policy to include the C&C policy. This example sets the trust-to-untrust zone.

```

root@host# set security policies from-zone trust to-zone untrust policy p2 match
source-address any destination-address any application any
root@host# set security policies from-zone trust to-zone untrust policy p2 then
permit application-services security-intelligence-policy cc_policy

```

6. Verify your command using the **show security policies** CLI command. It should look similar to this:

```

root@host# show security policies
...
from-zone trust to-zone untrust {
    policy p2 {
        match {
            source-address any;
            destination-address any;

```



```
        application any;
    }
    then {
        permit {
            application-services {
                security-intelligence-policy cc_policy;
            }
        }
    }
}
...
[edit]
```

7. Commit your changes.

#### RELATED DOCUMENTATION

| [Command and Control Servers: More Information](#) | 158

# File Scanning

## IN THIS CHAPTER

- [HTTP File Download Overview | 164](#)
- [HTTP File Download Details | 166](#)
- [Manual Scanning Overview | 169](#)
- [File Scanning Limits | 171](#)

## HTTP File Download Overview

Access this page from the **Monitor** menu.

A record is kept of all file metadata sent to the cloud for inspection. These are files downloaded by hosts and found to be suspicious based on known signatures or URLs. From the main page, click the file's signature to view more information, such as file details, what other malware scanners say about this file, and a complete list of hosts that downloaded this file.

### Benefits of viewing HTTP File Downloads

- Allows you to view a compiled list of suspicious downloaded files all in one place, including the signature, threat level, URL, and malware type.
- Allows you to filter the list of downloaded files by individual categories.

**Export Data**—Click the Export button to download file scanning data to a CSV file. You are prompted to narrow the data download to a selected time-frame.

The following information is available on this page.

**Table 39: HTTP Scanning Data Fields**

Field	Definition
File Signature	A unique identifier located at the beginning of a file that provides information on the contents of the file. The file signature can also contain information that ensures the original data stored in the file remains intact and has not been modified.

Table 39: HTTP Scanning Data Fields (continued)

Field	Definition
Threat Level	The threat score.  <b>NOTE:</b> Click the three vertical dots at the top of the column to filter the information on the page by threat level.
Filename	The name of the file, including the extension.  <b>NOTE:</b> Enter text in the space at the top of the column to filter the data.
Last Submitted	The time and date of the most recent scan of this file.
URL	The URL from which the file originated.  <b>NOTE:</b> Enter text in the space at the top of the column to filter the data.
Malware	The name of file and the type of threat if the verdict is positive for malware. Examples: Trojan, Application, Adware. If the file is not malware, the verdict is "clean."  <b>NOTE:</b> Enter text in the space at the top of the column to filter the data.
Category	The type of file. Examples: PDF, executable, document.  <b>NOTE:</b> Enter text in the space at the top of the column to filter the data.

## RELATED DOCUMENTATION

[Email Attachments Scanning Overview | 173](#)

[File Scanning Limits | 171](#)

[HTTP File Download Details | 166](#)

[Manual Scanning Overview | 169](#)

[Hosts Overview | 137](#)

[Host Details | 140](#)

[Telemetry Overview | 181](#)

## HTTP File Download Details

To access this page, navigate to **Monitor > File Scanning > HTTP File Download**. Click on the **File Signature** link to go to the File Scanning Details page.

Use this page to view analysis information and malware behavior summaries for the downloaded file. This page is divided into several sections:

**Table 40: Links on the HTTP File Download Details Page**

Button/Link	Purpose
Report False Positive	Click this button to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report, however, this does not change the verdict. If you want to make a correction (mark system as clean) you must do it manually.
Download STIX Report	<p>When there is a STIX report available, a download link appears on this page. Click the link to view gathered, open-source threat information, such as blacklisted files, addresses and URLs.</p> <p>STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties.</p> <p>STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing and consuming. Juniper Sky ATP uses this information as well as other sources. This occurs automatically. There is no administrator configuration required for STIX.</p> <p>STIX reports will vary. View a sample report at the bottom of this page.</p> <p><b>NOTE:</b> Juniper Sky ATP can also share threat intelligence. You can control what threat information is shared from the Threat Sharing page. See <a href="#">"Configuring Threat Intelligence Sharing" on page 119</a>.</p>
Download Zipped Files	(When available) Click this link to download the quarantined malware for analysis. The link allows you to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the General tab in the Juniper Sky ATP UI for the file in question.

Table 40: Links on the HTTP File Download Details Page (*continued*)

Button/Link	Purpose
Download PDF Report	Click this link to download a detailed report on the file in question. The report includes file threat level, protocol seen, file category and size, client IP address and username, and much more information, if available. This data is provided in a formatted PDF with a TOC.

The top of the page provides a quick view of the following information (scroll to the right in the UI to see more boxes):

- **Threat Level**—This is the threat level assigned (0-10), This box also provides the threat category and the action taken.
- **Top Indicators**—In this box, you will find the malware name, the signature it matches, and the IP address/URL from which the file originated.
- **Prevalence**—This box provides information on how often this malware has been seen, how many individual hosts on the network downloaded the file, and the protocol used.

## File Summary

Table 41: General Summary Fields

Field	Definition
Threat Level	This is the assigned threat level 0-10. 10 is the most malicious.
Action Taken	The action taken based on the threat level and host settings: block or permit.
Global Prevalence	How often this file has been seen across different customers.
Last Scanned	The time and date of the last scan to detect the suspicious file.
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe,, wordmui.msi.
Category	The type of file. Examples: PDF, executable, document.
File Size	The size of the downloaded file.
Platform	The target operating system of the file. Example. Win32
Malware Name	If possible, Juniper Sky ATP determines the name of the malware.

Table 41: General Summary Fields (continued)

Field	Definition
Malware Type	If possible, Juniper Sky ATP determines the type of threat. Example: Trojan, Application, Adware.
Malware Strain	If possible, Juniper Sky ATP determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio.
sha256 and md5	One way to determine whether a file is malware is to calculate a checksum for the file and then query to see if the file has previously been identified as malware.

In the Network Activity section, you can view information in the following tabs:

- **Contacted Domains**—If available, lists any domains that were contacted while executing the file in the Juniper Sky ATP sandbox.
- **Contacted IPs**—If available, lists all IPs that were contacted while executing the file, along with the destination IP's country, ASN, and reputation. The reputation field is based on Juniper IP intelligence data destination.
- **DNS Activity**— This tab lists DNS activity while executing the file, including reverse lookup to find the domain name of externally contacted servers. This tab also provides the known reputation of the destination servers.

## HTTP Downloads

This is a list of hosts that have downloaded the suspicious file. Click the **IP address** to be taken to the Host Details page for this host. Click the **Device Serial number** to be taken to the Devices page. From there you can view device versions and version numbers for the Juniper Sky ATP configuration, including profile, whitelist, and blacklist versions. You can also view the malware detection connection type for the device: telemetry, submission, or C&C event.

## Sample STIX Report

Figure 21: Sample STIX Report

```
<?xml version="1.0"?>
- <stix:STIX_Package version="1.2" id="example:Package-afbc14e2-b192-4ea0-848f-0a95aaea6cb3" xmlns:WinProcessObj="http://cybox.mitre.org/objects#WinProcessObject-2"
  xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2" xmlns:stix="http://stix.mitre.org/stix-1"
  xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1" xmlns:WinThreadObj="http://cybox.mitre.org/objects#WinThreadObject-2" xmlns:example="http://example.com"
  xmlns:stixCommon="http://stix.mitre.org/common-1" xmlns:cybox="http://cybox.mitre.org/cybox-2" xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
  xmlns:ttp="http://stix.mitre.org/TTP-1" xmlns:xlink="http://www.w3.org/1999/xlink" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2" xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
  xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2" xmlns:indicator="http://stix.mitre.org/Indicator-2" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
- <stix:STIX_Header>
  <stix:Description>IOCs for sample id: a9c097d0f6392897ff87764d43ac9ad4b60078f7062325b7798909e484f31af</stix:Description>
</stix:STIX_Header>
- <stix:Indicators>
  <stix:Indicator id="example:indicator-92000f82-82b0-45bf-9ac7-bf4566c1c93d" xsi:type="indicator:IndicatorType" timestamp="2017-10-09T20:31:25.918941+00:00">
    <indicator:Title>File Indicator(s) for sample:a9c097d0f6392897ff87764d43ac9ad4b60078f7062325b7798909e484f31af</indicator:Title>
    <indicator:Description>An indicator containing File observable(s)</indicator:Description>
    <indicator:Observable id="example:Observable-987ee5c7-6c56-414c-a696-f3199d5aa0fb">
      <cybox:Object id="example:File-4f1c86c5-725b-4d44-b19e-e1787dc05c28">
        <cybox:Properties xsi:type="FileObj:FileObjectType">
          <FileObj:Hashes>
            <cyboxCommon:Hash>
              <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0">MD5</cyboxCommon:Type>
              <cyboxCommon:Simple_Hash_Value>b941993d05adf34dc9b7d35fe3f0ae61</cyboxCommon:Simple_Hash_Value>
            </cyboxCommon:Hash>
            <cyboxCommon:Hash>
              <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA1</cyboxCommon:Type>
              <cyboxCommon:Simple_Hash_Value>e70f1bb911ee60ef6e7aa2c423eaa5a04d17e709</cyboxCommon:Simple_Hash_Value>
            </cyboxCommon:Hash>
            <cyboxCommon:Hash>
              <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256</cyboxCommon:Type>
              <cyboxCommon:Simple_Hash_Value>a9c097d0f6392897ff87764d43ac9ad4b60078f7062325b7798909e484f31af</cyboxCommon:Simple_Hash_Value>
            </cyboxCommon:Hash>
            <cyboxCommon:Hash>
              <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA512</cyboxCommon:Type>
              <cyboxCommon:Simple_Hash_Value>1afc3d6e068c8e3bb617726a0ecdec428da99c874ef2f1c98538651b6d537bf5e8d00a0e2c49b2d20740146c9ef5f77</cyboxCommon:Simple_Hash_Value>
            </cyboxCommon:Hash>
          </FileObj:Hashes>
        </cybox:Properties>
      </cybox:Object>
    </indicator:Observable>
  </stix:Indicator>
</stix:Indicators>
```

## RELATED DOCUMENTATION

[File Scanning Limits | 171](#)

[HTTP File Download Overview | 164](#)

[Manual Scanning Overview | 169](#)

[Hosts Overview | 137](#)

## Manual Scanning Overview

Access this page from the **Monitor** menu.

If you suspect a file is suspicious, you can manually upload it to the cloud for scanning and evaluation. Click the **Manual Upload** button to browse to the file you want to upload. The file can be up to 32 MB.

### Benefits of Manually Scanning Files

- Allows you to investigate files that weren't filtered by existing blacklists.
- Provides all file analysis data that accompanies known suspicious files, such as behavior analysis and network activity.

There is a limit to the number of files administrators can upload for manual scanning. File uploads are limited by realm (across all users in a realm) in a 24-hour period. You can upload two files per each active device enrolled and 10 files per each premium-licensed device in your account. For example, if you have two Juniper Sky ATP premium-licensed SRX Series devices and one other SRX Series device, Juniper Sky ATP will allow a maximum of 22 files to be allowed in a 24-hour window.

**NOTE:** You must have an SRX Series device registered with Juniper Sky ATP in order to use the manual file scanning feature.

**Table 42: File Scanning Data Fields**

Field	Definition
File Signature	A unique identifier located at the beginning of a file that provides information on the contents of the file. The file signature can also contain information that ensures the original data stored in the file remains intact and has not been modified.
Threat Level	The threat score.
Filename	The name of the file, including the extension.
Last Submitted	The time and date of the most recent scan of this file.
URL	The URL from which the file originated.
Verdict	The name of file and the type of threat if the verdict is positive for malware. Examples: Trojan, Application, Adware. If the file is not malware, the verdict is "clean."
Category	The type of file. Examples: PDF, executable, document.

## RELATED DOCUMENTATION

[Hosts Overview | 137](#)

[HTTP File Download Overview | 164](#)

[HTTP File Download Details | 166](#)

[Email Attachments Scanning Overview | 173](#)

[Email Attachments Scanning Details | 174](#)



## File Scanning Limits

There is a limit to the number of files which can be submitted to the cloud for inspection. This limit is dictated by the device and license type. When the limit is reached, the file submission process is paused.

**NOTE:** This limit applies to all files, HTTP and SMTP.

Limit thresholds operate on a sliding scale and are calculated within 24-hour time-frame starting "now."

Perimeter Device	Free License (files per day)	Premium License (files per day)
SRX340	200	1,000
SRX345	300	2,000
SRX550m	500	5,000
SRX1500	2,500	10,000
SRX4100	3000	20000
SRX4200	3000	35000
SRX4600	5,000	60,000
SRX5400	5,000	50,000
SRX5600	5,000	70,000
SRX5800	5,000	100,000
vSRX(10mbps)	25	200
vSRX(100mbps)	200	1,000
vSRX(1000mbps)	2,500	10,000
vSRX(2000mbps)	2,500	10,000
vSRX(4000mbps)	3,000	20,000

## RELATED DOCUMENTATION

[HTTP File Download Overview | 164](#)

---

[Email Attachments Scanning Overview | 173](#)

---

[Manual Scanning Overview | 169](#)

# Email Scanning

## IN THIS CHAPTER

- [Email Attachments Scanning Overview | 173](#)
- [Email Attachments Scanning Details | 174](#)
- [SMTP Quarantine Overview: Blocked Emails | 177](#)
- [IMAP Block Overview | 179](#)

## Email Attachments Scanning Overview

Access this page from the **Monitor** menu.

A record is kept of all file metadata sent to the cloud for inspection. These are files downloaded by hosts and found to be suspicious based on known signatures. From the main page, click the file's signature to view more information, such as file details, what other malware scanners say about this file, and a complete list of hosts that downloaded this file.

### Benefits of Viewing Scanned Email Attachments

- Allows you to view a compiled list of suspicious email attachments all in one place, including the file hash, threat level, file name, and malware type.
- Allows you to filter the list of email attachments by individual categories.

**Export Data**—Click the Export button to download file scanning data to a CSV file. You are prompted to narrow the data download to a selected time-frame.

The following information is available on this page.

**Table 43: Email Attachments Scanning Data Fields**

Field	Definition
File Signature	A unique identifier located at the beginning of a file that provides information on the contents of the file. The file signature can also contain information that ensures the original data stored in the file remains intact and has not been modified.

Table 43: Email Attachments Scanning Data Fields (continued)

Field	Definition
Threat Level	The threat score.
Date Scanned	The date and time the file was scanned.
Filename	The name of the file, including the extension.
Recipient	The email address of the intended recipient.
Sender	The email address of the sender.
Malware Name	The type of malware found.
Status	Indicates whether the file was blocked or permitted.
Category	The type of file. Examples: PDF, executable, document.

## RELATED DOCUMENTATION

[Email Attachments Scanning Details | 174](#)

[File Scanning Limits | 171](#)

[HTTP File Download Overview | 164](#)

[HTTP File Download Details | 166](#)

[Hosts Overview | 137](#)

[Host Details | 140](#)

[Telemetry Overview | 181](#)

## Email Attachments Scanning Details

To access this page, navigate to **Monitor > File Scanning > Email Attachments**. Click on the **File Signature** to go to the File Scanning Details page.

Use this page to view analysis information and malware behavior summaries for the downloaded file. This page is divided into several sections:

**Report False Positives**—Click the **Report False Positive** button to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report, however, this does not change the verdict. If you want to make a correction (mark system as clean) you must do it manually.

#### **Download STIX Report**—

When there is a STIX report available, a download link appears on this page. Click the link to view gathered, open-source threat information, such as blacklisted files, addresses and URLs. STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties.

STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing and consuming. Juniper Sky ATP uses this information as well as other sources. This occurs automatically. There is no administrator configuration required for STIX.

**NOTE:** Juniper Sky ATP can also share threat intelligence. You can control what threat information is shared from the Threat Sharing page. See [“Configuring Threat Intelligence Sharing” on page 119](#).

**Download Zipped Files**—(When available) Click this link to download the quarantined malware for analysis. The link allows you to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the General tab in the Juniper Sky ATP UI for the file in question.

The top of the page provides a quick view of the following information (scroll to the right in the UI to see more boxes):

- **Threat Level**—This is the threat level assigned (0-10), This box also provides the threat category and the action taken.
- **Top Indicators**—In this box, you will find the malware name, the signature it matches, and the IP address/URL from which the file originated.
- **Prevalence**—This box provides information on how often this malware has been seen, how many individual hosts on the network downloaded the file, and the protocol used.

## File Summary

Table 44: General Summary Fields

Field	Definition
Threat Level	This is the assigned threat level 0-10. 10 is the most malicious.
Action Taken	The action taken based on the threat level and host settings: block or permit.
Global Prevalence	How often this file has been seen across different customers.
Last Scanned	The time and date of the last scan to detect the suspicious file.
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe,, wordmui.msi.
Category	The type of file. Examples: PDF, executable, document.
File Size	The size of the downloaded file.
Platform	The target operating system of the file. Example. Win32
Malware Name	If possible, Juniper Sky ATP determines the name of the malware.
Malware Type	If possible, Juniper Sky ATP determines the type of threat. Example: Trojan, Application, Adware.
Malware Strain	If possible, Juniper Sky ATP determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio.
sha256 and md5	One way to determine whether a file is malware is to calculate a checksum for the file and then query to see if the file has previously been identified as malware.

In the Network Activity section, you can view information in the following tabs:

**NOTE:** This section will appear blank if there has been no network activity.

- **Contacted Domains**—If available, lists any domains that were contacted while executing the file in the Juniper Sky ATP sandbox.

- **Contacted IPs**—If available, lists all IPs that were contacted while executing the file, along with the destination IP's country, ASN, and reputation. The reputation field is based on Juniper IP intelligence data destination.
- **DNS Activity**— This tab lists DNS activity while executing the file, including reverse lookup to find the domain name of externally contacted servers. This tab also provides the known reputation of the destination servers.

In the Behavior Details section, you can view the behavior of the file on the system. This includes any processes that were started, files that were dropped, and network activity seen during the execution of the file. Dropped files are any additional files that were downloaded and installed by the original file.

## RELATED DOCUMENTATION

[HTTP File Download Overview | 164](#)

[HTTP File Download Details | 166](#)

[Email Attachments Scanning Overview | 173](#)

[Manual Scanning Overview | 169](#)

[SMTP Quarantine Overview: Blocked Emails | 177](#)

## SMTP Quarantine Overview: Blocked Emails

Access this page from the **Monitor** menu.

The SMTP quarantine monitor page lists quarantined emails with their threat score and other details including sender and recipient. You can also take action on quarantined emails here, including releasing them and adding them to the blacklist.

The following information is available from the Summary View:

**Table 45: Blocked Email Summary View**

Field	Description
Time Range	Use the slider to narrow or increase the time-frame within the selected the time parameter in the top right: 12 hrs, 24 hrs, 7 days or custom.
Total Email Scanned	This lists the total number of emails scanned during the chosen time-frame and then categorizes them into blocked, quarantined, released, and permitted emails.

Table 45: Blocked Email Summary View (continued)

Field	Description
Malicious Email Count	This is a graphical representation of emails, organized by time, with lines for blocked emails, quarantined and not released emails, and quarantined and released emails.
Emails Scanned	This is a graphical representation of emails, organized by time, with lines for total emails, and emails with one or more attachments.
Email Classification	This is another graphical view of classified emails, organized by percentage of blocked emails, quarantined and not released emails, and quarantined and released emails.

The following information is available from the Details View:

Table 46: Blocked Email Details View

Field	Description
Recipient	The email address of the recipient.
Sender	The email address of the sender.
Subject	Click the <b>Read This</b> link to go to the Juniper Sky ATP quarantine portal and preview the email.
Date	The date the email was received.
Malicious Attachment	Click on the attachment name to go to the Juniper Sky ATP file scanning page where you can view details about the attachment.
Size	The size of the attachment in kilobytes.
Threat Score	The threat score of the attachment, 0-10, with 10 being the most malicious.
Threat Name	The type of threat found in the attachment, for example, worm or trojan.
Action	The action taken, including the date and the person (recipient or administrator) who took the action.

Using the available buttons on the Details page, you can take the following actions on blocked emails:

- Add domain to blacklist



- Add sender to blacklist
- Release

## RELATED DOCUMENTATION

[Email Management Overview | 65](#)

[Email Management: Configure SMTP | 67](#)

[Creating Whitelists and Blacklists | 59](#)

[HTTP File Download Overview | 164](#)

## IMAP Block Overview

Access this page from the **Monitor > Email Quarantine** menu.

The IMAP Block monitor page lists blocked emails with their threat score and other details including sender and recipient. You can also take action on blocked emails here, including releasing them and adding them to the blacklist.

The following information is available from the Summary View:

**Table 47: Blocked Email Summary View**

Field	Description
Time Range	Use the slider to narrow or increase the time-frame within the selected the time parameter in the top right: 12 hrs, 24 hrs, 7 days or custom.
Malicious Email Count	This lists the total number of malicious emails scanned during the chosen time-frame and then categorizes them into blocked, blocked and not allowed, quarantined and allowed.
Emails Scanned	This is a graphical representation of all scanned emails, organized by date.

The following information is available from the Detail View:

**Table 48: Blocked Email Detail View**

Field	Description
Recipient	The email address of the recipient.

Table 48: Blocked Email Detail View (continued)

Field	Description
Sender	The email address of the sender.
Subject	Click the <b>Read This</b> link to go to the Juniper Sky ATP quarantine portal and preview the email.
Date	The date the email was received.
Malicious Attachment	Click on the attachment name to go to the Juniper Sky ATP file scanning page where you can view details about the attachment.
Size	The size of the attachment in kilobytes.
Threat Score	The threat score of the attachment, 0-10, with 10 being the most malicious.
Threat Name	The type of threat found in the attachment, for example, worm or trojan.
Action	The action taken, including the date and the person (recipient or administrator) who took the action.

Using the available buttons on the Details page, you can take the following actions on blocked emails:

- Unblock Attachment for Selected User(s)
- Unblock Attachment for All Users

#### RELATED DOCUMENTATION

[Email Management: Configure IMAP | 70](#)

[Email Management Overview | 65](#)

# Telemetry

## IN THIS CHAPTER

- [Telemetry Overview | 181](#)
- [Telemetry Details | 183](#)

## Telemetry Overview

**NOTE:** Telemetry support is available starting in Junos OS 17.4R1.

Access this page from the **Monitor > Telemetry > Web Protocols** or **Email Protocols** menu.

The telemetry page provides comprehensive monitoring information of devices for a variety of activities, including the number of web and email files scanned or blocked per protocol. It also offers a counter reset capability.

### Benefits of Telemetry

- Exposes monitoring data in the Juniper Sky ATP web portal that was previously only accessible from the SRX Series device via CLI.
- Centralizes valuable monitoring data in one place, facilitating the ability to put events in context against other events for a more comprehensive view of the network.

**Reset** button—When you select the check box for a device and click Reset, it clears the counter to zero for that device and protocol. This reset applies only to the information displayed on the web portal.

For the Devices listed on this page, you can view the following information for Web Protocols by selecting the HTTP tab and the HTTPS tab.

Table 49: Telemetry Data for Web Protocols

Web Protocols	Available Data
HTTP and HTTPS	Device Name—Click on the device name to open the telemetry details page for the device.
	Total Scanned
	Blocked
	Permitted
	Ignored
	Blacklist hits
	Whitelist hits
	Last Reset (This is the time when the device counter was last reset to zero. Note that the reset applies only to the information that is displayed on the web portal.)

For the Devices listed on this page, you can view the following information for Email Protocol by selecting the tabs that correspond to SMTP, SMTPS, IMAP, and IMAPS.

Table 50: Telemetry Data for Email Protocols

Email Protocols	Available Data
SMTP and SMTPS IMAP and IMAPS	Device Name—Click on the device name to open the telemetry details page for the device.
	Total Scanned
	Blocked
	Permitted
	Ignored
	Blacklist hits
	Whitelist hits
	Last Reset (This is the time when the device counter was last reset to zero. Note that the reset applies only to the information that is displayed on the web portal.)

## RELATED DOCUMENTATION

[Telemetry Details | 183](#)

[HTTP File Download Overview | 164](#)

[Email Attachments Scanning Overview | 173](#)

## Telemetry Details

To access this page, navigate to **Monitor > Telemetry > Web Protocols** or **Email Protocols > <Protocol> tab ><Device Name>**. Click on the device name link for any available device to access the details page.

Use this page to view device, connection, and configuration version information. Refer to the tables below for a list of data points available on this page.

**Table 51: Device Information**

Field	Definition
Device Name	Host name of the SRX Series device
Model Number	SRX Series device model number
Serial Number	SRX Series device serial number
OS Version	SRX Series device JunOS version
Submission State	Allowed or Paused. This indicates whether the device can submit files to Juniper Sky ATP or if it has reached its daily limit. (At this time, the limit is 10,000 files per day for premium accounts.)

**Table 52: Connection Updated**

Field	Definition
Submission	The month, date, year, and time when data was received for this connection type.
C&C Event	
Telemetry	

Table 53: Configuration Version - Device and Cloud

List Name	Device	Cloud
Global Config	These fields indicate the version numbers of each list, both on the device and in the cloud. You can compare them to see if they are in sync.	
Profile Config		
Global Whitelist		
Global Blacklist		
Customer Whitelist		
Customer Blacklist		

#### RELATED DOCUMENTATION

[Telemetry Overview | 181](#)

[HTTP File Download Details | 166](#)

[Email Attachments Scanning Details | 174](#)

# Encrypted Traffic Analysis

## IN THIS CHAPTER

- [Encrypted Traffic Analysis Overview | 185](#)
- [Encrypted Traffic Analysis Details | 189](#)

## Encrypted Traffic Analysis Overview

Access this page from the **Monitor > Encrypted Traffic** menu.

Encrypted traffic analysis helps you to detect malicious threats that are hidden in encrypted traffic without intercepting and decrypting the traffic.

### Benefits of encrypted traffic analysis

- Monitors network traffic for threats without breaking the encryption of the traffic, thereby adhering to data privacy laws.
- Erases the need for additional hardware or network changes to set up and manage the network:
  - The SRX Series device provides the required metadata (such as known malicious certificates and connection details) and connection patterns to Sky ATP cloud.
  - The Sky ATP cloud provides behavior analysis and machine learning capabilities.
- Provides greater visibility and policy enforcement over encrypted traffic without requiring resource-intensive SSL decryption:
  - Based on the network behaviors analyzed by Sky ATP cloud, the network connections are classified as malicious or benign.
- Adds an additional layer of protection beyond traditional information security solutions to help organizations reduce and manage risk.
- Ensures no latency as we do not decrypt the traffic.

[Table 54 on page 186](#) lists the information that is available on the Encrypted Traffic Analysis page.

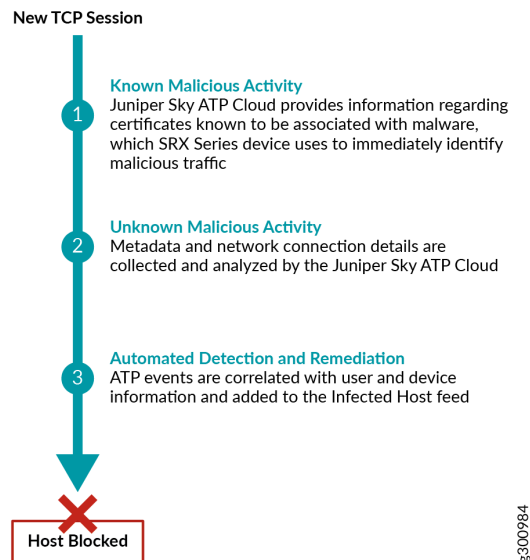
Table 54: Encrypted Traffic Analysis

Field	Guideline
External Server IP	The IP address of the external server.
External Server Hostname	The host name of the external server.
Highest Threat Level	The threat level on the external server based on encrypted traffic analysis.
Count	The number of times hosts on the network have attempted to contact this server.
Country	The country where the external server is located.
Last Seen	The date and time of the most recent external server hit.
Category	Additional category information known about this server, for example, botnets, malware, etc.

### Encrypted Traffic Analysis and Detection

The encrypted traffic analysis combines rapid response and network analysis (both static and dynamic) to detect and remediate malicious activity hidden in encrypted sessions. [Figure 22 on page 186](#) shows the staged approach for encrypted traffic analysis.

Figure 22: Encrypted Traffic Analysis and Detection



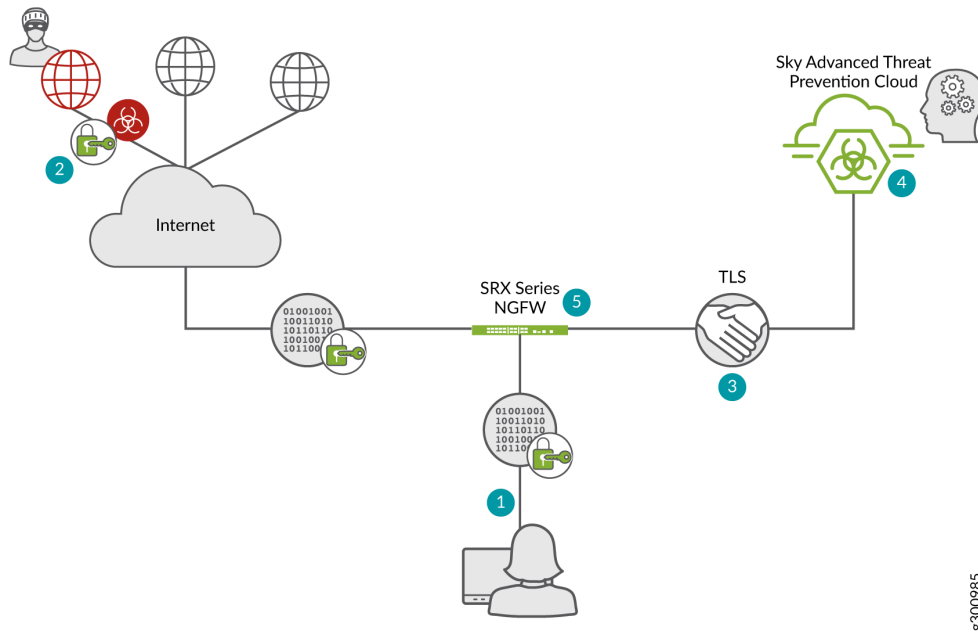


**Workflow**

This section provides the topology and workflow to perform encrypted traffic analysis.

Figure 23 on page 187 shows the logical topology of encrypted traffic analysis workflow.

**Figure 23: Topology for encrypted traffic analysis**



Step	Description
1	A client host, who is located behind an SRX Series device requests a file to be downloaded from the Internet.
2	The SRX series device receives the response from the Internet. The SRX series device extracts the server certificate from the session and compares its signature with the blacklist certificate signatures. If a match occurs, then connection is blocked.  <b>NOTE:</b> The Juniper Networks Sky ATP Cloud feed keeps the SRX device up to date with a feed of certificates associated with known malware sites.
3	The SRX device collects the metadata and connection statistics and sends it to the Sky ATP cloud for analysis.
4	The Sky ATP cloud performs behavioral analysis to classify the traffic as benign or malicious.

Step	Description
5	If a malicious connection is detected, the threat score of the host is recalculated. If the new score is above the threshold, then the client host is added to infected host list, The client host might be blocked based on policy configurations on SRX Series devices.

## Configurations on SRX Series Devices

To enable encrypted traffic analysis on SRX Series devices, include the following CLI configurations:

1. Configure the security-metadata-streaming policy.

```
set services security-metadata-streaming policy policy-name http action permit
set services security-metadata-streaming policy policy-name http notification log
```

2. Attach the security-metadata-streaming policy to a security firewall policy.

```
set security policies from-zone zone-name to-zone zone-name application-services
security-metadata-streaming-policy policy-name
```

Use the **show services security-metadata-streaming statistics** command to view the statistics of security metadata streaming policy.

**show services security-metadata-streaming statistics**

```
user@host> show services security-metadata-streaming statistics
```

```
Security Metadata Streaming session statistics:
  Session inspected:      10
  Session whitelisted:    0
  Session detected:       6

Security Metadata Streaming submission statistics:
  Records submission success:      8
  Records submission failure:      2
```

To view the list of servers that are whitelisted for encrypted traffic analysis, use the **show services security-metadata-streaming whitelist** command.

**show services security-metadata-streaming whitelist**

```
user@host> show services security-metadata-streaming whitelist
```

```
No. IP-start IP-end Feed Address
1 192.0.5.0 192.0.5.1 eta_custom_whitelist ID-80001400
```

## RELATED DOCUMENTATION

[Encrypted Traffic Analysis Details](#) | 189

## Encrypted Traffic Analysis Details

To access this page, navigate to **Monitor > Encrypted Traffic**. Click on any of the **External Server IP** address links.

Use the Encrypted Traffic Analysis Details page to view analysis information and a threat summary for the external server. The following information is displayed for each server:

- Total Hits
- Threat Summary (Location, Category, Time last seen)
- Ports and protocols used

The encrypted traffic analysis details page is divided into several sections:

[Table 55 on page 189](#) lists the actions that you can perform on this page. You can perform these actions using the options that are available on the upper right corner of the page.

**Table 55: Options on the Encrypted Traffic Analysis Details Page**

Button/Link	Purpose
Select Option > Add to Whitelist	Choose this option to whitelist the server from encrypted traffic analysis based detections.  <b>NOTE:</b> You can also whitelist the servers from the <b>Configure &gt; Whitelists &gt; ETA</b> page.
Select Option > Report False Positive	Choose this option to send a report to Juniper Networks, informing Juniper of a false positive. Juniper will investigate the report; however, this does not change the verdict.

Under Time Range is a graph displaying the frequency of events over time. An event occurs when a host communicates to the external server IP address (either sending or receiving data). You can filter this information by clicking on the timeframe links: 1 day, 1 week, 1 month, Custom (select your own time-frame).

**Hosts** is a list of hosts that have contacted the external server. [Table 56 on page 190](#) lists the information provided in this section.

**Table 56: External Server Contacted Host Data**

Field	Definition
Client Host	The name of the host in contact with the external server.
Client IP Address	The IP address of the host in contact with the external server. (Click through to the Host Details page for this host IP address.)
Threat Level at Time	The threat level of the external server as determined by an analysis of actions and behaviors at the time of the event.
Status	The action taken by the device on the communication (whether it was permitted or blocked).  <b>NOTE:</b> At this point of time, encrypted traffic analysis only detects malicious threats but does not block it. Actions such as blocking is handled by features such as infected hosts based on the host threat score and customer policies.
Protocol	The protocol (https) the external server used to attempt communication.
Source Port	The port the external server used to attempt communication.
Uploaded	Number of bytes uploaded to the server.
Downloaded	Number of bytes downloaded from the server.
Device Name	The name of the SRX device in contact with the external server.
Date/Time Seen	The date and time of the most recent external server hit.
Username	The name of the host user in contact with the external server.

Select a client host and click **Download packet** to download the packet capture details and view more information about the network/SSL traffic.

**Domains** is a list of domains that the IP address has previously used at the time of suspicious events. If an external IP address is seen changing its DNS/domain name to evade detection, a list of the various names used will be listed along with the dates in which they were seen.

Table 57: External Server Associated Domains Data

Field	Definition
C&C Host	This is a list of domains the destination IP addresses in the external server events resolved to.
Last Seen	The date and time of the most recent external server hit.

**Signatures** is a list of the threat indicators associated with the IP address.

Table 58: ETA Server Signature Data

Field	Definition
Name	The name or type of detected malware.
Category	Description of the malware and way in which it may have compromised a resource or resources.
Date	The date the malware was seen.

**Certificates** is a list of certificates associated with the external server. Click **View Certificate** and **Download Certificate**

Table 59: ETA Server Certificate Data

Field	Definition
Subject	Specifies the IP address of the external server.
Issuer	Specifies the authority that issued the certificate.
SHA1	SHA1 hash of the server certificate.
Date/Time Seen	The date and time when the SHA1 file was last updated.

## RELATED DOCUMENTATION

| [Encrypted Traffic Analysis Overview](#) | 185

# 5

PART

## Policies on the SRX Series Device

---

[Configure Juniper Sky ATP Policies on the SRX Series Device](#) | **193**

[Configure IP-Based Geolocations on the SRX Series Device](#) | **206**

---

# Configure Juniper Sky ATP Policies on the SRX Series Device

## IN THIS CHAPTER

- Juniper Sky Advanced Threat Prevention Policy Overview | 193
- Enabling Juniper Sky ATP for Encrypted HTTPS Connections | 196
- Example: Configuring a Juniper Sky Advanced Threat Prevention Policy Using the CLI | 197
- Unified Policies | 202
- Explicit Web Proxy Support | 204

## Juniper Sky Advanced Threat Prevention Policy Overview

The connection to the Juniper Sky ATP cloud is launched on-demand. It is established only when a condition is met and a file or URL must be sent to the cloud. The cloud inspects the file and returns a verdict number (1 through 10). A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the Juniper Sky ATP policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

Juniper Sky ATP policies are an extension to the Junos OS security policies. [Table 60 on page 194](#) shows the additions.

**NOTE:** Starting in Junos OS Release 15.1X49-D80, the match-then condition has been deprecated from the Juniper Sky ATP policy configuration. For more information, see [Juniper Sky Advanced Threat Prevention Release Notes for Junos 15.1X49-D80](#). The examples below are for Junos OS Release 15.1X49-D80 and later.

Table 60: Juniper Sky ATP Security Policy Additions

Addition	Description
Action and notification based on the verdict number and threshold	<p>Defines the threshold value and what to do when the verdict number is greater than or equal to the threshold. For example, if the threshold is 7 (the recommended value) and Juniper Sky ATP returns a verdict number of 8 for a file, then that file is blocked from being downloaded and a log entry is created.</p> <pre>set services advanced-anti-malware policy aamwpolicy1 verdict-threshold recommended set services advanced-anti-malware policy aamwpolicy1 http action block notification log</pre>
Default action and notification	<p>Defines what to do when the verdict number is less than the threshold. For example, if the threshold is 7 and Juniper Sky ATP returns a verdict number of 3 for a file, then that file is downloaded and a log file is created.</p> <pre>set services advanced-anti-malware policy aamwpolicy1 default-notification log</pre>
Name of the inspection profile	<p>Name of the Juniper Sky ATP profile that defines the types of file to scan.</p> <pre>set services advanced-anti-malware policy aamwpolicy1 http inspection-profile default_profile</pre>
Fallback options	<p>Defines what to do when error conditions occur or when there is a lack of resources. The following fallback options are available:</p> <ul style="list-style-type: none"> <li>• action—Permit or block the file regardless of its threat level.</li> <li>• notification—Add or do not add this event to the log file.</li> </ul> <pre>set services advanced-anti-malware policy aamwpolicy1 fallback-options action permit set services advanced-anti-malware policy aamwpolicy1 fallback-options notification log</pre> <p><b>NOTE:</b> The above actions assume a valid session is present. If no valid session is present, Juniper Sky ATP permits the file, regardless of whether you set the fallback option to block.</p>
Blacklist notification	<p>Defines whether to create a log entry when attempting to download a file from a site listed in the blacklist file.</p> <pre>set services advanced-anti-malware policy aamwpolicy1 blacklist-notification log</pre>



Table 60: Juniper Sky ATP Security Policy Additions (*continued*)

Addition	Description
Whitelist notification	<p>Defines whether to create a log entry when attempting to download a file from a site listed in the whitelist file.</p> <pre>set services advanced-anti-malware policy aamwpolicy1 whitelist-notification log</pre>
Name of smtp inspection profile	<p>Name of the inspection profile for SMTP email attachments. The “actions to take” are defined in the Web UI and not through CLI commands.</p> <pre>set services advanced-anti-malware policy aamwpolicy1 smtp inspection-profile my_smtp_profile</pre>

Use the **show services advanced-anti-malware policy** CLI command to view your Juniper Sky ATP policy settings.

```
user@host> show services advanced-anti-malware policy aamwpolicy1
Advanced-anti-malware configuration:
Policy Name: aamwpolicy1
  Default-notification   : No Log
  Whitelist-notification: Log
  Blacklist-notification: Log
  Fallback options:
    Action: permit
    Notification: Log
  Protocol: HTTP
  Verdict-threshold: recommended (7)
    Action: block
    Notification: Log
  Inspection-profile: default_profile
  Protocol: SMTP
  Verdict-threshold: recommended (7)
    Action: User-Defined-in-Cloud (permit)
    Notification: No Log
  Inspection-profile: my_smtp_profile
```

Use the **show security policies** CLI command to view your firewall policy settings.

```
user@host# show security policies
from-zone trust to-zone untrust {
  policy 1 {
```

```

match {
    source-address any;
    destination-address any;
    application any;
}
then {
    permit {
        application-services {
            security-intelligence-policy SecIntel;
        }
    }
}
}
policy firewall-policy1 {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit {
            application-services {
                ssl-proxy {
                    profile-name ssl-inspect-profile;
                }
                advanced-anti-malware-policy aamwpolicy1;
            }
        }
    }
}
}
}

```

For more examples, see [“Example: Configuring a Juniper Sky Advanced Threat Prevention Policy Using the CLI”](#) on page 197.

## Enabling Juniper Sky ATP for Encrypted HTTPS Connections

If you have not already done so, you need to configure `ssl-inspect-ca` which is used for ssl forward proxy and for detecting malware in HTTPS. Shown below is just one example for configuring ssl forward proxy. For complete information, see [Configuring SSL Proxy](#).

1. From operational mode, generate a PKI public/private key pair for a local digital certificate.

```
user@host > request security pki generate-key-pair certificate-id certificate-id size size type type
```

For example:

```
user@host > request security pki generate-key-pair certificate-id ssl-inspect-ca size 2048 type rsa
```

2. From operational mode, define a self-signed certificate. Specify certificate details such as the certificate identifier (generated in the previous step), a fully qualified domain name for the certificate, and an e-mail address of the entity owning the certificate.

```
user@host > request security pki local-certificate generate-self-signed certificate-id certificate-id
domain-name domain-name subject subject email email-id
```

For example:

```
user@host > request security pki local-certificate generate-self-signed certificate-id ssl-inspect-ca
domain-name www.juniper.net subject "CN=www.juniper.net,OU=IT,O=Juniper
Networks,L=Sunnyvale,ST=CA,C=US" email security-admin@juniper.net
```

Once done, you can configure the SSL forward proxy to inspect HTTPs traffic. For example:

```
user@host# set services ssl proxy profile ssl-inspect-profile root-ca ssl-inspect-ca
user@host# set security policies from-zone trust to-zone untrust policy
firewall-policy1 then permit application-services ssl-proxy profile-name
ssl-inspect-profile
```

For a more complete example, see [“Example: Configuring a Juniper Sky Advanced Threat Prevention Policy Using the CLI” on page 197](#).

## RELATED DOCUMENTATION

| [Example: Configuring a Juniper Sky Advanced Threat Prevention Policy Using the CLI | 197](#)

## Example: Configuring a Juniper Sky Advanced Threat Prevention Policy Using the CLI

### IN THIS SECTION

- [Requirements | 198](#)
- [Overview | 198](#)

- Configuration | 199
- Verification | 202

This example shows how to create a Juniper Sky ATP policy using the CLI. It assumes you understand configuring security zones and security policies. See [Example: Creating Security Zones](#).

## Requirements

This example uses the following hardware and software components:

- An SRX1500 device with traffic through packet forwarding.
- Junos OS Release 15.1X49-D80 or later.

**NOTE:** Starting in Junos OS Release 15.1X49-D80, the match-then condition has been deprecated from the Juniper Sky ATP policy configuration. For more information, see [Juniper Sky Advanced Threat Prevention Release Notes for Junos 15.1X49-D80](#). This example includes those updates.

**NOTE:** Junos OS Release 18.2R1 or later adds explicit web proxy support for anti-malware and security-intelligence policies using the following statements: **set services advanced-anti-malware connection proxy-profile proxy\_name** and **set services security-intelligence proxy-profile proxy\_name**. First use the set services command to configure the web proxy profile, including the proxy host IP address and port number. See [“Explicit Web Proxy Support” on page 204](#) for details.

## Overview

This example creates a Juniper Sky ATP policy that has the following properties:

- Policy name is aamwpolicy1.
- Profile name is default\_profile.
- Block any file if its returned verdict is greater than or equal to 7 and create a log entry.
- Do not create a log entry if a file has a verdict less than 7.

- When there is an error condition, allow files to be downloaded and create a log entry.
- Create a log entry when attempting to download a file from a site listed in the blacklist or whitelist files.

## **Configuration**

### **Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see [Using the CLI Editor in Configuration Mode](#) in the Junos OS CLI User Guide.

**NOTE:** Starting in Junos OS Release 15.1X49-D80, the **match-then** condition has been deprecated from the Juniper Sky ATP policy configuration. Configurations made prior to 15.1X49-D80 will continue to work but it is recommended you do not use these statements going forward. For more information, see [Juniper Sky ATP Release Notes \(for Junos 15.1X49-D80\)](#).

1. Create the Juniper Sky ATP policy.

- Set the policy name to `aamwpolicy1` and block any file if its returned verdict is greater than or equal to 7.

```
user@host# set services advanced-anti-malware policy aamwpolicy1 verdict-threshold 7
```

- Associate the policy with the `default_profile` profile.

```
user@host# set services advanced-anti-malware policy aamwpolicy1 http inspection-profile default_profile
```

- Block any file if its returned verdict is greater than or equal to 7 and create a log entry.

```
user@host# set services advanced-anti-malware policy aamwpolicy1 http action block notification log
```

- When there is an error condition, allow files to be downloaded and create a log entry.

```
user@host# set services advanced-anti-malware policy aamwpolicy1 fallback-options action permit
user@host# set services advanced-anti-malware policy aamwpolicy1 fallback-options notification log
```

- Create a log entry when attempting to download a file from a site listed in the blacklist or whitelist files.

```
user@host# set services advanced-anti-malware policy aamwpolicy1 blacklist-notification log
user@host# set services advanced-anti-malware policy aamwpolicy1 whitelist-notification log
```

- For smtp, you only need to specify the profile name. The user-defined action-to-take is defined in the Juniper Sky ATP cloud portal.

```
user@host# set services advanced-anti-malware policy aamwpolicy1 smtp inspection-profile my_smtp_profile
```

2. Configure the firewall policy to enable the advanced anti-malware application service.

```
user@host# set security policies from-zone trust to-zone untrust policy
firewall-policy1 match source-address any
user@host# set security policies from-zone trust to-zone untrust policy
```

```

firewall-policy1 match destination-address any
user@host# set security policies from-zone trust to-zone untrust policy
firewall-policy1 match application any
user@host# set security policies from-zone trust to-zone untrust policy
firewall-policy1 then permit application-services advanced-anti-malware
aamwpolicy1

```

### 3. Configure the SSL proxy profile to inspect HTTPs traffic.

```

user@host# set services ssl proxy profile ssl-inspect-profile root-ca
ssl-inspect-ca

```

### 4. Configure the SSL forward proxy to inspect HTTPs traffic.

Note that this command assumes you have already configured `ssl-inspect-ca` which is used for ssl forward proxy. If you have not already done so, an error occurs when you commit this configuration. See [“Enabling Juniper Sky ATP for Encrypted HTTPS Connections” on page 196](#) for more information on configuring `ssl-inspect-ca`.

```

user@host# set security policies from-zone trust to-zone untrust policy
firewall-policy1 then permit application-services ssl-proxy profile-name
ssl-inspect-profile

```

### 5. Review your policy. It should look similar to this.

```

user@root> show services advanced-anti-malware policy
Advanced-anti-malware configuration:
Policy Name: aamwpolicy1
  Default-notification   : No Log
  Whitelist-notification: Log
  Blacklist-notification: Log
  Fallback options:
    Action: permit
    Notification: Log
  Protocol: HTTP
    Verdict-threshold: 7
    Action: block
    Notification: Log
    Inspection-profile: default_profile
  Protocol: SMTP
    Verdict-threshold: 7

```

```
Action: User-Defined-in-Cloud (permit)
Notification: No Log
Inspection-profile: my_smtp_profile
```

## Verification

### *Verifying That the Policy Is Working*

#### Action

First, verify that your SRX Series device is connected to the cloud.

```
show services advanced-anti-malware status
```

Next, clear the statistics to make it easier to read your results.

```
clear services advanced-anti-malware statistics
```

After some traffic has passed through your SRX Series device, check the statistics to see how many sessions were permitted, blocked, and so forth according to your profile and policy settings.

```
show services advanced-anti-malware statistics
```

## Unified Policies

Starting in Junos OS Release 18.2R1, unified policies are supported on SRX Series devices, allowing granular control and enforcement of dynamic Layer 7 applications within the traditional security policy. See the Junos 18.2R1 documentation for more details on Unified Policies.

### Overview

**NOTE:** This overview is taken from the SRX Series documentation. The commands listed here are specific to Juniper Sky ATP, but for a detailed explanation of unified policies and how they work, you should refer to the Junos documentation.



Unified policies are security policies where you can use dynamic applications as match conditions, along with existing 5-tuple or 6-tuple matching conditions, to detect application changes over time, and allow you to enforce a set of rules for the transit traffic. Unified policies allow you to use dynamic applications as one of the policy match criteria in each application.

By adding dynamic application to the matching conditions, the data traffic is classified based on the Layer 7 application inspection results. AppID identifies dynamic or real-time Layer 4-Layer 7 applications, and after a particular application is identified, actions are performed as per the security policy. (Before identifying the final application, if the policy cannot be matched precisely, a potential policy list is made available, and the traffic is permitted using the potential policy from the list.) After the application is identified, the final policy is applied to the session. Policy actions such as permit, deny, reject, or redirect is applied on the traffic as per the policy rules.

Juniper Sky ATP is supported for unified policies. The **set services security-intelligence default-policy** and **set services advanced-anti-malware default-policy** commands are introduced to create default policies for each. During the initial policy lookup phase, which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list, which contain different security intelligence or anti-malware policies, the SRX Series device applies the default policy until a more explicit match has occurred.

Here are the possible completions for the security intelligence default-policy:

```
root@host# set services security-intelligence default-policy ?
Possible completions:
<category>           Name of security intelligence category
+ apply-groups        Groups from which to inherit configuration data
+ apply-groups-except Don't inherit configuration data from these groups
description           Text description of policy
```

Here are the possible completions for the anti malware default-policy:

```
root@host# set services advanced-anti-malware default-policy ?
Possible completions:
<[Enter]>           Execute this command
+ apply-groups        Groups from which to inherit configuration data
+ apply-groups-except Don't inherit configuration data from these groups
> blacklist-notification Blacklist notification logging option
> default-notification Notification action taken for action
> fallback-options    Fallback options for abnormal conditions
> http                Configure HTTP options
> imap                Configure IMAP options
> smtp                Configure SMTP options
verdict-threshold    Verdict threshold
```

```
> whitelist-notification Whitelist notification logging option
|                               Pipe through a command
```

## Explicit Web Proxy Support

With release Junos OS 18.2R1, you can configure explicit web proxy support for SRX Series services Juniper Sky ATP connections.

If your network uses a web proxy for access and authentication for HTTP(S) outbound sessions, you can configure your Juniper Sky ATP connections on the SRX Series device to go through a specified web proxy host. To configure HTTP(S) connections to use a web proxy, you create one or more proxy profiles and refer to those profiles in your anti-malware and security intelligence policies.

**NOTE:** Support starting in Junos OS 18.2R1.

Note that authentication to the proxy host is not supported in this release. Therefore a whitelist rule may be needed for the proxy host, with no authentication for Juniper Sky ATP tunnel traffic.



**WARNING:** If you are using a web proxy, you must enroll SRX Series devices using a slightly different process, as follows:

For the first part, get the enrollment op script from the Juniper Sky ATP Web UI like you normally would.

1. Click the **Enroll** button on the **Devices** page.
2. Copy the command to your clipboard and click **OK**.
3. Take only the URL portion (none of the text in front of it) and enter it into the Junos OS CLI of the SRX Series device you want to enroll using the following command:
 

```
> request services advanced-anti-malware enroll https://amer.Juniper
Sky.junipersecurity.net/v1/skyatp/ui_api/bootstrap/enroll/5vhcfia9y18nn98v/k2ygewjwm6c0ap4s.slax
```
4. Press **Enter**. (Note that this command must be run in operational mode.)

On the SRX Series device, use the `set services` command to set the web proxy profile by entering the proxy host IP address and port number as follows:

```
set services proxy profile proxy_name protocol http host x.x.x.x port xxxx
```

Add the web proxy profile you created to your Juniper Sky ATP policies using the following commands:

```
set services advanced-anti-malware connection proxy-profile proxy_name
set services security-intelligence proxy-profile proxy_name
```

Use the **show services advanced-anti-malware status** command to view the web proxy IP address and port number. For example:

```
root@argon-host> show services advanced-anti-malware status
Server connection status:
  Server hostname: srxapi.dep4.test.testsystem.net
Server port: 443
+ Proxy hostname: x.x.x.x
+ Proxy port: 3128
  Control Plane:
    Connection time: 2018-5-02 17:03:09 PDT
    Connection status: Connected.
  Service Plane:
    fpc0
    Connection active number: 12
    Connection retry statistics: 0
```

## RELATED DOCUMENTATION

| [Example: Configuring a Juniper Sky Advanced Threat Prevention Policy Using the CLI](#) | 197

# Configure IP-Based Geolocations on the SRX Series Device

## IN THIS CHAPTER

- [Geolocation IPs and Juniper Sky Advanced Threat Prevention | 206](#)
- [Configuring Juniper Sky Advanced Threat Prevention With Geolocation IP | 207](#)

## Geolocation IPs and Juniper Sky Advanced Threat Prevention

IP-based Geolocation (GeoIP) is a mapping of an IP address to the geographic location of an Internet connected to a computing device. Juniper Sky Advanced Threat Prevention supports GeoIP, giving you the ability to filter traffic to and from specific geographies in the world.

**NOTE:** Currently you configure GeoIP through CLI commands and not through the Web interface.

GeoIP uses a Dynamic Address Entry (DAE) infrastructure. A DAE is a group of IP addresses, not just a single IP prefix, that can be imported into Juniper Sky Advanced Threat Prevention from external sources. These IP addresses are for specific domains or for entities that have a common attribute such as a particular undesired location that poses a threat. The administrator can then configure security policies to use the DAE within a security policy. When the DAE is updated, the changes automatically become part of the security policy. There is no need to update the policy manually.

The cloud feed URL is set up automatically for you when you run the op script to configure your SRX Series device. See [“Downloading and Running the Juniper Sky Advanced Threat Prevention Script” on page 24](#).

Currently, configuring GeoIP and security policies is done completely on the SRX Series device using CLI commands.

## RELATED DOCUMENTATION

| [Configuring Juniper Sky Advanced Threat Prevention With Geolocation IP | 207](#)

## Configuring Juniper Sky Advanced Threat Prevention With Geolocation IP

To configure Juniper Sky ATP with GeoIP, you first create the GeoIP DAE and specify the interested countries. Then, create a security firewall policy on the SRX Series device to reference the DAE and define whether to allow or block access.

To create the GeoIP DAE and security firewall policy:

1. Create the DAE using the **set security dynamic-address** CLI command. Set the category to **GeoIP** and property to **country** (all lowercase). When specifying the countries, use the two-letter ISO 3166 country code in capital ASCII letters; for example, US or DE. For a complete list of country codes, see [ISO 3166-1 alpha-2](#).

In the following example, the DAE name is **my-geoip** and the interested countries are the United States (US) and Great Britain (GB).

```
root@host# set security dynamic-address address-name my-geoip profile category
GeoIP property country string US
root@host# set security dynamic-address address-name my-geoip profile category
GeoIP property country string GB
```

2. Use the **show security dynamic-address** CLI command to verify your settings. Your output should look similar to the following:

```
root@host# show security dynamic-address
address-name my-geoip {
  profile {
    category GeoIP {
      property country {
        string US;
        string GB;
      }
    }
  }
}

[edit]
```

3. Create the security firewall policy using the **set security policies** CLI command.

In the following example, the policy is from the untrust to trust zone, the policy name is **my-geoip-policy**, the source address is **my-geoip** created in Step 1, and the action is to deny access from the countries listed in **my-geoip**.

```
root@host# set security policies from-zone untrust to-zone trust policy
my-geoip-policy match source-address my-geoip destination-address any application
any
root@host# set security policies from-zone untrust to-zone trust policy
my-geoip-policy then deny
```

4. Use the **show security policies** CLI command to verify your settings. Your output should look similar to the following:

```
root@host# show security policies
...
from-zone untrust to-zone trust {
  policy my-geoip-policy {
    match {
      source-address my-geoip;
      destination-address any;
      application any;
    }
    then {
      deny;
    }
  }
}
...
```

## RELATED DOCUMENTATION

[Geolocation IPs and Juniper Sky Advanced Threat Prevention](#) | 206



# Administration

---

Juniper Sky ATP Administration | **210**

---

# Juniper Sky ATP Administration

## IN THIS CHAPTER

- [Modifying My Profile | 210](#)
- [Creating and Editing User Profiles | 211](#)
- [Application Tokens Overview | 213](#)
- [Creating Application Tokens | 213](#)
- [Multi-Factor Authentication Overview | 215](#)
- [Configure Multi-Factor Authentication for Administrators | 215](#)

## Modifying My Profile

An administrator profile is created for you when you register for a Juniper Sky ATP account. Use this page at any time to edit your administrator profile. You can also change your password from this page.

- Note that your username must be a valid e-mail address.
- If you are changing your password, make sure you understand the syntax requirements.
- Note that the administrator profile is only for the web UI. It does not grant access to any SRX Series device.

To update your administrator profile, do the following:

1. Select **Administration**. This takes you to the My Profile landing page.
2. Edit the fields described in the table below.
3. Click **OK** to save your changes or click **Reset** to discard them.

**NOTE:** To change only your password, click **Change Password**.



Table 61: My Profile Fields

Setting	Guideline
First Name	Enter a string beginning with an alphanumeric character.
Last Name	Enter a string beginning with an alphanumeric character.
E-mail	Enter a valid e-mail address.
Password	Enter a unique string at least 8 characters long. Include both uppercase and lowercase letters, at least one number, and at least one special character (~!@#\$%^&*()_-=+{}[] :;<>.,/?); no spaces are allowed, and you cannot use the same sequence of characters that are in your username. Note that your username for Juniper Sky ATP is your e-mail address.
Role Assignment	Change the role assignment: System administrator, Operator, or Observer
MFA Method	<p>If multi-factor authentication is enabled, this field displays the verification method, Mobile SMS or Email.</p> <p>If this user is locked out for too many verification code requests, click the link to <b>Reset mobile number</b>. This removes the lock, allowing the user to step through the Verification Identity screen again.</p> <p>Note that there is no way to remove a lockout if the MFA method is Email.</p>

## RELATED DOCUMENTATION

[Creating and Editing User Profiles | 211](#)

[Reset Password | 38](#)

## Creating and Editing User Profiles

Use this page to create additional user accounts or modify existing accounts for Juniper Sky ATP. Multiple users can log into Juniper Sky ATP at the same time.

- Review the [“Modifying My Profile” on page 210](#) topic.
- Note that if multiple administrators are editing the same window at the same time, the last session to save their settings overwrites the other session’s changes.

To add additional administrator accounts:

1. Select **Administration > Users**.
2. Enter the information described in the table below.
3. Click **OK**.

**Table 62: User Fields**

Setting	Guideline
First Name	Enter a string beginning with an an alphanumeric character.
Last Name	Enter a string beginning with an an alphanumeric character.
E-mail Address	Enter a valid e-mail address.
Role Assignment	<p>You can assign different roles to users to determine their level of access to configurations. When you create a user, select their role from the pulldown. Available roles are:</p> <ul style="list-style-type: none"> <li>• <b>System Administrator</b>—A system administrator has full write access to the Juniper Sky ATP web portal and can edit all configuration information. Only a system administrator can create and edit user accounts.</li> <li>• <b>Operator</b>—An operator has write access to the Juniper Sky ATP web portal and can edit all configuration information with the exception of user accounts.</li> <li>• <b>Observer</b>—An observer has read-access only to the Juniper Sky ATP web portal with the exception of user accounts.</li> </ul>
Password	Enter a unique string at least 8 characters long. Include both uppercase and lowercase letters, at least one number, and at least one special character (~!@#\$\$%^&*()_ -+={}[] :;<>.,/?); no spaces are allowed, and you cannot use the same sequence of characters that are in your username. Note that your username for Juniper Sky ATP is your e-mail address.
Confirm Password	Re-enter the password.

## RELATED DOCUMENTATION

Modifying My Profile | 210

## Application Tokens Overview

Use the Application Token page to view or add application tokens that allow Security Director or Open API users to securely access Juniper Sky ATP APIs over HTTPS. Using the available buttons, you can mark tokens as active or inactive.

When a token is used, you can view the IP address of the user and the date of last usage by clicking the token name. Then you can block or unblock IP addresses that are trying to use individual tokens. An application token is marked inactive if it has not been used for 30 days. Once inactive, all access using the token is blocked until it is activated again. If an application token has not been used for 90 days, it is automatically deleted and cannot be recovered again.

### Benefits of Application Tokens

- Limits the applications that can use Juniper Sky ATP APIs and Juniper Sky ATP threat information to only those that are authorized. For example, you can limit who has access to your shared threat information by creating an application token for TAXII. See [“Configuring Threat Intelligence Sharing” on page 119](#).
- Allows you to easily activate or deactivate a token from one central location.

### RELATED DOCUMENTATION

| [Creating Application Tokens](#) | 213

## Creating Application Tokens

To access this page, click **Administration** > **Application Tokens**. You can generate application tokens from the App Tokens page.

- Review the [“Application Tokens Overview” on page 213](#) topic.
- Note that an application token is marked inactive if it has not been used for 30 days. Once inactive, all access using the token is blocked until it is activated again. If an application token has not been used for 90 days, it is automatically deleted and cannot be recovered again.
- Note that when you generate an application token, you must copy and paste it at the time of generation. Once you close the generation screen, the token is no longer available for copying.

To generate an application token:

1. Select **Administration** > **Application Tokens**.
2. Click the plus (+) icon.
3. Complete the configuration by using the guidelines in [Table 63 on page 214](#) below.
4. Click **OK**.
5. Copy and paste the generated token into the Open API configuration process by using it as the bearer token in the authorization header.



**WARNING:** When you generate an application token, you must copy and paste it at the time of generation. Once you close the generation screen, the token is no longer available for copying.

**Table 63: Application Token Settings**

Field	Description
Name	Enter a unique name for this token. This must be a unique string that only contains, letters, numbers, and dashes; no spaces allowed; 32-character maximum.
Description	Enter a description for your token; maximum length is 1024 characters. You should make this description as useful as possible for all administrators.
Access Type	Select one or both check boxes to generate an application token for Security Director and/or Third Party feeds.

When you generate a token, it is active by default. To deactivate a token or activate it again:

1. Select the check box beside the application token.
2. Click the **Deactivate** button. Use the **Activate** button to reinstate the token after it's deactivated.

When you click an application token name, you can view the IP addresses of devices that have used the token and the time the token was utilized. To block and IP address or unblock it:

1. Select the check box beside the IP address.
2. Click the **Block** button. Use the **Unblock** button to reinstate access to the IP address.

## RELATED DOCUMENTATION

[Application Tokens Overview | 213](#)

[Command and Control Servers Overview | 153](#)

## Multi-Factor Authentication Overview

Multi-Factor Authentication requires a user to pass at least two different types of authentication before gaining access to a requested page. Juniper Sky ATP lets you configure multi-factor authentication (over SMS or Email) for administrators who are logging into the Juniper Sky ATP Web UI or resetting their passwords. This is an optional setting that when enabled, applies globally to all administrators in a realm.

The benefits of multi-factor authentication are:

- Improves security by minimizing the chances of unauthorized access to resources.
- Adds authentication layers with the ability to randomize login credentials and mitigate danger when user passwords are compromised.
- Allows systems to verify the identity of the user by contacting that user directly, thereby alerting the user to unauthorized access if he or she did not initiate the login request.

When you enable multi-factor authentication, you select to send a verification code by text or email when administrators attempt to login to Juniper Sky ATP. The first time administrators try to login, they are prompted to enter their mobile number. Once that information is entered, they can receive a verification code. Once the code is entered and verified, the user can login the Juniper Sky ATP Web UI.

## RELATED DOCUMENTATION

[Configure Multi-Factor Authentication for Administrators | 215](#)

## Configure Multi-Factor Authentication for Administrators

### IN THIS SECTION

- [Enable Multi-Factor Authentication | 216](#)
- [Verification Codes for Multi-Factor Authentication: Mobile SMS | 217](#)

- Verification Codes for Multi-Factor Authentication: Email | 217
- Unlock a User | 218

## Enable Multi-Factor Authentication

When you enable multi-factor authentication for a realm, it is turned on for all administrators in at realm. You must be a System Administrator to enable multi-factor authentication.

To enable and configure multi-factor authentication settings, navigate to **Administration > Multifactor Authentication**.

1. Use the slider to enable multifactor authentication.
2. Select an authentication method. This is the method by which a verification code will be sent to the administrator, either **Mobile SMS** or **Email**.

If you select Email, the configuration is finished, and you can click **Save**. Sky ATP will use the email address already entered for each user. If you select Mobile SMS, continue to the next step.

**NOTE:** A user is locked out of Sky ATP for 1 hour if 4 verification codes have been sent without any being used (verified) to login to Sky ATP.

**NOTE:** When you change the authentication method, if any users have been locked out due to too many verification code requests, those users are all automatically unlocked. All counters that track the number of verification codes that have been sent are reset to zero when the authentication method is changed.

3. Select an **Expiration Interval**. The options are:
  - Every time user logs in—User must enter a verification code for every log in.
  - Every day—Multi-factor authentication is required every 24 hours. After going through the multi-factor authentication process once, only username and password are required to log in until 24 hours have passed.

- Every week—Every week—Multi-factor authentication is required every 7 days. After going through the multi-factor authentication process once, only username and password are required to log in until 7 days have passed.
- Month— Multi-factor authentication is required every 30 days. After going through the multi-factor authentication process once, only username and password are required to log in until 30 days have passed.

**NOTE:** The user can select a check box on the Verify Identity screen to remember the code for the period of time selected above. If the user does not click the check box, she will have to go through the verification process again no matter what expiration interval is configured.

4. Click **Save**.

### Verification Codes for Multi-Factor Authentication: Mobile SMS

When Mobile SMS is set as the authentication method, the first time an administrator attempts to log in to the Juniper Sky ATP Web UI (enters a username and password), a Verify Identity screen appears. Administrators must enter the following information in the Verify Identity screen:

- Select the country where the mobile number was issued.
- Enter their mobile phone number (numbers only, no dashes or other characters)
- Click the **Send Code** button. A verification code is sent to the mobile device.
- Once the code is received by text or email, enter the 8 digit code in the Verification Code field.
- Click **Verify**.

Lockout Conditions: If an administrator does not receive the code, she can click the Send Code button again. Note the following security precautions in place for resending code requests: Sky ATP will wait 60 seconds after sending a code before it will send another code once a request is made. Once a user has requested a verification code 4 times without logging in to Sky ATP, she is permanently locked out. In this case, the user must contact an administrator to remove the lock.

### Verification Codes for Multi-Factor Authentication: Email

When Email is set as the authentication method, the first time an administrator attempts to log in to the Juniper Sky ATP Web UI (by entering a username and password), a Verify Identity screen appears. Users must enter the following information:

- Enter the 8 digit verification code contained in the email.
- Click **Verify**.

If a user does not receive the code, she should check her spam folder. If it's not there, she can click the Resend Code button. Note the following security precautions about resending code requests. Sky ATP will wait 60 seconds after sending a code before it will send another code once a request is made. Once a user has requested a verification code 4 times without logging in to Sky ATP, she is locked out for 1 hour, meaning a new code cannot be requested for that amount of time.

**NOTE:** When Email is the MFA method, the one hour lockout cannot be cleared. The user must wait the full hour before requesting another verification code.

## Unlock a User

An SMS lockout can be removed by a system administrator who is logged into Juniper Sky ATP.

To remove the lockout,

1. Navigate to **Administration** > **Users** and locate the locked out user.
2. Select the check box to edit the user.
3. On the User Edit screen is MFA Method and Mobile Number. Click the link to **Reset mobile number**. This removes the lock, allowing the user to step through the Verification Identity screen again, and the code request counter is reset to zero.

## RELATED DOCUMENTATION

| [Multi-Factor Authentication Overview | 215](#)



# 7

PART

## Troubleshoot

---

Troubleshooting Topics | 220

---

# Troubleshooting Topics

## IN THIS CHAPTER

- [Juniper Sky Advanced Threat Prevention Troubleshooting Overview | 220](#)
- [Troubleshooting Juniper Sky Advanced Threat Prevention: Checking DNS and Routing Configurations | 221](#)
- [Troubleshooting Juniper Sky Advanced Threat Prevention: Checking Certificates | 224](#)
- [Troubleshooting Juniper Sky Advanced Threat Prevention: Checking the Routing Engine Status | 226](#)
- [request services advanced-anti-malware data-connection | 228](#)
- [request services advanced-anti-malware diagnostic | 230](#)
- [Troubleshooting Juniper Sky Advanced Threat Prevention: Checking the application-identification License | 234](#)
- [Viewing Juniper Sky Advanced Threat Prevention System Log Messages | 235](#)
- [Configuring traceoptions | 236](#)
- [Viewing the traceoptions Log File | 238](#)
- [Turning Off traceoptions | 238](#)
- [Juniper Sky Advanced Threat Prevention Dashboard Reports Not Displaying | 239](#)
- [Juniper Sky Advanced Threat Prevention RMA Process | 240](#)

## Juniper Sky Advanced Threat Prevention Troubleshooting Overview

This topic provides a general guide to troubleshooting some typical problems you may encounter on Juniper Sky ATP.

[Table 64 on page 221](#) provides a summary of the symptom or problem and recommended actions with links to the troubleshooting documentation.

Table 64: Troubleshooting Juniper Sky ATP

Symptom or Problem	Recommended Action
SRX device can't communicate with cloud	<p>See <a href="#">“Troubleshooting Juniper Sky Advanced Threat Prevention: Checking DNS and Routing Configurations”</a> on page 221</p> <p>See <a href="#">“Troubleshooting Juniper Sky Advanced Threat Prevention: Checking Certificates”</a> on page 224</p> <p>See <a href="#">“Troubleshooting Juniper Sky Advanced Threat Prevention: Checking the Routing Engine Status”</a> on page 226</p> <p>See <a href="#">request services advanced-anti-malware data-connection</a></p> <p>See <a href="#">request services advanced-anti-malware diagnostic</a></p>
Files not being sent to cloud	<p>See <a href="#">“Troubleshooting Juniper Sky Advanced Threat Prevention: Checking DNS and Routing Configurations”</a> on page 221</p> <p>See <a href="#">“Troubleshooting Juniper Sky Advanced Threat Prevention: Checking Certificates”</a> on page 224</p> <p>See <a href="#">“Troubleshooting Juniper Sky Advanced Threat Prevention: Checking the Routing Engine Status”</a> on page 226</p> <p>See <a href="#">“Troubleshooting Juniper Sky Advanced Threat Prevention: Checking the application-identification License”</a> on page 234</p>
Viewing system log messages	See <a href="#">“Viewing Juniper Sky Advanced Threat Prevention System Log Messages”</a> on page 235
Setting traceoptions	<p>See <a href="#">“Configuring traceoptions”</a> on page 236</p> <p>See <a href="#">“Viewing the traceoptions Log File”</a> on page 238</p> <p>See <a href="#">“Turning Off traceoptions”</a> on page 238</p>
Dashboard reports not displaying any data	See <a href="#">“Juniper Sky Advanced Threat Prevention Dashboard Reports Not Displaying”</a> on page 239

## Troubleshooting Juniper Sky Advanced Threat Prevention: Checking DNS and Routing Configurations

Domain name system (DNS) servers are used for resolving hostnames to IP addresses.

For redundancy, it is a best practice to configure access to multiple DNS servers. You can configure a maximum of three DNS servers. The approach is similar to the way Web browsers resolve the names of a Web site to its network address. Additionally, Junos OS enables you configure one or more domain names, which it uses to resolve hostnames that are not fully qualified (in other words, the domain name is missing). This is convenient because you can use a hostname in configuring and operating Junos OS without the need to reference the full domain name. After adding DNS server addresses and domain names to your Junos OS configuration, you can use DNS resolvable hostnames in your configuration and commands instead of IP addresses.

DNS servers are site-specific. The following presents examples of how to check your settings. Your results will be different than those shown here.

First, check the the IP addresses of your DNS servers.

```
user@host# show groups global system name-server
xxx.xxx.x.68;
xxx.xxx.xx.131;
```

If you set up next-hop, make sure it points to the correct router.

```
user@host# show routing-options
static {
    route 0.0.0.0/0 next-hop xx.xxx.xxx.1;
```

```
user@host# show groups global routing-options
static {
    route xxx.xx.0.0/12 {
        next-hop xx.xxx.xx.1;
        retain;
        no-readvertise;
    }
}
```

Use ping to verify the SRX Series device can communication with the cloud server. First use the **show services advanced-anti-malware status** CLI command to get the cloud server hostname.

```
user@host> show service advanced-anti-malware status
Server connection status:
    Server hostname: xxx.xxx.xxx.com
```

```

Server port: 443
Control Plane:
  Connection Time: 2015-12-14 00:08:10 UTC
  Connection Status: Connected
Service Plane:
  fpc0
  Connection Active Number: 0
  Connection Failures: 0

```

Now ping the server. Note that the cloud server will not respond to ping, but you can use this command to check that the hostname can be resolved to the IP address.

```
user@host>ping xxx.xxx.xxx.com
```

If you do not get a **ping: cannot resolve hostname: Unknown host** message, then the hostname can be resolved.

You can also use telnet to verify the SRX Series device can communicate to the cloud server. First, check the routing table to find the external route interface. In the following example, it is **ge-0/0/3.0**.

```

user@host> show route
inet.0: 23 destinations, 23 routes (22 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[Static/5] 2d 17:42:53
                   > to xx.xxx.xxx.1 via ge-0/0/3.0

```

Now telnet to the cloud using port 443.

```

telnet xxx.xxx.xxx.xxx.com port 443 interface ge-0/0/3.0
Trying xx.xxx.xxx.119...
Connected to xxx.xxx.xxx.xxx.com
Escape character is '^]'

```

If telnet is successful, then your SRX Series device can communicate with the cloud server.

## Troubleshooting Juniper Sky Advanced Threat Prevention: Checking Certificates

Use the **show security pki local-certificate** CLI command to check your local certificates. Ensure that you are within the certificate's valid dates. The **ssl-inspect-ca** certificate is used for SSL proxy. Show below are some examples. Your output may look different as these are dependent on your setup and location.

```

user@host> show security pki local-certificate
Certificate identifier: ssl-inspect-ca
  Issued to: www.juniper_self.net, Issued by: CN = www.juniper_self.net, OU = IT
, O = Juniper Networks, L = xxxxx, ST = xxxxx, C = IN
  Validity:
    Not before: 11-24-2015 22:33 UTC
    Not after: 11-22-2020 22:33 UTC
  Public key algorithm: rsaEncryption(2048 bits)

Certificate identifier: argon-srx-cert
  Issued to: xxxx-xxxx_xxx, Issued by: C = US, O = Juniper Ne
tworks Inc, OU = SecIntel, CN = SecIntel (junipersecurity.net) subCA for SRX dev
ices, emailAddress = xxx@juniper.net
  Validity:
    Not before: 10-30-2015 21:56 UTC
    Not after: 01-18-2038 15:00 UTC
  Public key algorithm: rsaEncryption(2048 bits)

```

Use the **show security pki ca-certificate** command to check your CA certificates. The **argon-ca** certificate is the client certificate's CA while the **argon-secintel-ca** is the server certificate's CA. Ensure that you are within the certificate's valid dates.

```

root@host> show security pki ca-certificate
Certificate identifier: argon-ca
  Issued to: SecIntel (junipersecurity.net) subCA for SRX devices, Issued by: C
= US, O = Juniper Networks Inc, OU = SecIntel, CN = SecIntel (junipersecurity.ne
t) CA, emailAddress = xxx@juniper.net
  Validity:
    Not before: 05-19-2015 22:12 UTC
    Not after: 05- 1-2045 15:00 UTC
  Public key algorithm: rsaEncryption(2048 bits)

Certificate identifier: argon-secintel-ca
  Issued to: SecIntel (junipersecurity.net) CA, Issued by: C = US, O = Juniper N

```

```

etworks Inc, OU = SecIntel, CN = SecIntel (junipersecurity.net) CA, emailAddress
= xxx@juniper.net
Validity:
  Not before: 05-19-2015 03:22 UTC
  Not after: 05-16-2045 03:22 UTC
Public key algorithm: rsaEncryption(2048 bits)

```

When you enroll an SRX Series device, the ops script installs two CA certificates: one for the client and one for the server. Client-side CA certificates are associated with serial numbers. Use the **show security pki local-certificate detail** CLI command to get your device's certificate details and serial number.

```

user@host> show security pki local-certificate detail
Certificate identifier: aamw-srx-cert
Certificate version: 3
Serial number: xxxxxxxxxxxx
Issuer:
  Organization: Juniper Networks Inc, Organizational unit: SecIntel, Country:
US,
  Common name: SecIntel (junipersecurity.net) subCA for SRX devices
Subject:
  Organization: xxxxxxxxxxxx, Organizational unit: SRX, Country: US,
  Common name: xxxxxxxxxxxx
Subject string:
  C=US, O=xxxxxxxxxx, OU=SRX, CN=xxxxxxxxxx, emailAddress=secintel-ca@juniper.net
Alternate subject: secintel-ca@juniper.net, fqdn empty, ip empty
Validity:
  Not before: 11-23-2015 23:08 UTC
  Not after: 01-18-2038 15:00 UTC

```

Then use the **show security pki crl detail** CLI command to make sure your serial number is not in the Certificate Revocation List (CRL). If your serial number is listed in the CRL then that SRX Series device cannot connect to the cloud server.

```

user@host> show security pki crl detail
CA profile: aamw-ca
CRL version: V00000001
CRL issuer: C = US, O = Juniper Networks Inc, OU = SecIntel, CN = SecIntel
(junipersecurity.net) subCA for SRX devices, emailAddress = secintel-ca@juniper.net

Effective date: 11-23-2015 23:16 UTC
Next update: 11-24-2015 23:16 UTC

```

```

Revocation List:
  Serial number          Revocation date
  xxxxxxxxxxxxxxxxxxxxxx 10-26-2015 17:43 UTC
  xxxxxxxxxxxxxxxxxxxxxx 11- 3-2015 19:07 UTC
  ...

```

## Troubleshooting Juniper Sky Advanced Threat Prevention: Checking the Routing Engine Status

Use the **show services advanced-anti-malware status** CLI command to show the connection status from the control plane or routing engine.

```

user@host> show services advanced-anti-malware status
Server connection status:
  Server hostname: xxx.xxx.xxx.xxx.com
  Server port: 443
  Control Plane:
    Connection Time: 2015-12-01 08:58:02 UTC
    Connection Status: Connected
  Service Plane:
    fpc0
    Connection Active Number: 0
    Connection Failures: 0

```

If the connection fails, the CLI command will display the reason in the Connection Status field. Valid options are:

- Not connected
- Initializing
- Connecting
- Connected
- Disconnected
- Connect failed
- Client certificate not configured
- Request client certificate failed



- Request server certificate validation failed
- Server certificate validation succeeded
- Server certificate validation failed
- Server hostname lookup failed

## request services advanced-anti-malware data-connection

### Syntax

```
request services advanced-anti-malware data-connection test (start <0-32768> | status)
```

### Release Information

Command introduced in Junos OS Release 15.1X49-D60.

### Description

Tests the connection between the SRX Series device and the Juniper Sky ATP cloud by initiating a websocket connection and then sending data payloads of a given size. The SRX Series device must already be enrolled with Juniper Sky ATP before running this command.

Run this command when the **show services advanced-anti-malware statistics** CLI command shows that several files failed to be sent to the cloud (see the “File Send to Cloud Failed” result.)

### Options

**start <0-32768>**—Start the data connection test and specify the packet payload size in bytes.

**status**—Returns the result of the data connection test. See [Table 65 on page 229](#).

### Required Privilege Level

View

## RELATED DOCUMENTATION

[request services advanced-anti-malware diagnostic](#) | 230

### List of Sample Output

[request services advanced-anti-malware data-connection test start on page 229](#)

[request services advanced-anti-malware data-connection test status on page 229](#)

[request services advanced-anti-malware data-connection test status on page 229](#)

### Output Fields

This CLI command returns a single line that indicates the data connection results. [Table 65 on page 229](#) lists the possible results.

Table 65: Data Connection Test Output

Message	Description
Test not started.	You cannot view the status without first running the data connection test. Run the <b>request services advanced-anti-malware data-connection test start</b> CLI command and then check the status again.
Test in progress.	The data connection test has not finished. Wait a few seconds and try the command again.  Depending on your environment, it can take up to 20 seconds for the test to complete.
Test OK.	The data connection test passed.
Test failed.	The data connection test failed and indicates where it failed. Possible failures are: <ul style="list-style-type: none"> <li>• Connect error—The websocket connection cannot be established.</li> <li>• Ping pong error—Successfully connected to the cloud server, but the payload delivery is not reliable.</li> </ul>

## Sample Output

**request services advanced-anti-malware data-connection test start**

```
user@host> request services advanced-anti-malware data-connection test start
```

```
Cloud connectivity test started. Ping payload size: 128 bytes.
```

**request services advanced-anti-malware data-connection test status**

```
user@host> request services advanced-anti-malware data-connection test status
```

```
fpc0: Test OK. RTT = 38 ms. Test time: 2016-08-11 20:53:02 UTC.
```

**request services advanced-anti-malware data-connection test status**

```
user@host> request services advanced-anti-malware data-connection test status
```

```
fpc0: Test failed. Reason: Ping pong error. Test time: 2016-08-11 21:13:05 UTC.
```

## request services advanced-anti-malware diagnostic

### Syntax

```
request services advanced-anti-malware diagnostic url (detail | pre-detection url | routing-instance instance-name)
```

### Release Information

Command introduced in Junos OS Release 15.1X49-D60. The interface name to cloud check, MTU warning, and client and server clock check added in Junos OS Release 15.1X49-D90. **routing-instance** option added in Junos OS Release 15.1X49-D100.

### Description

Use this command before you enroll your SRX Series device with Juniper Sky Advanced Threat Prevention to verify your Internet connection to the cloud. If you already enrolled your SRX Series device, you can still use this command and the **request services aamw data-connection** CLI command to check and troubleshoot your connection to the cloud.

This CLI command checks the following:

- DNS lookup—Performs a forward DNS lookup of the cloud hostname to verify it returns an IP address. The examining process is aborted if it cannot get an interface name to the cloud. This issue may be caused by a connection error. Please check your network connection.
- Route to cloud—Tests your network connection using telnet.
- Whether server is live—Uses the telnet and ping commands to verify connection with the cloud.
- Outgoing interface—Checks that both the Routing Engine (RE) and the Packet Forwarding Engine (PFE) can connect to the Internet.
- IP path MTU—Determines the maximum transmission unit (MTU) size on the network path between the SRX Series device and the cloud server. The examining process is aborted if the outgoing interface MTU is less than 1414. As a workaround, set the outgoing interface MTU to the default value or to a value greater than 1414.

A warning message appears if the path MTU is less than the outgoing interface MTU. This is a minor issue and you can ignore the message. A higher path MTU is recommended but a low path MTU will work.

- SSL configuration consistency—Verifies that the SSL profile, client certificate and CA exists in both the RE and the PFE.
- Client and server clock check—When you run this CLI command, it first checks the difference between the server time and the local time. The time difference is expected to be less than one minute. If the time difference is more than one minute, an error message is displayed. See [Table 66 on page 231](#).

### Options

**url**—URL to the Juniper Sky Advanced Threat Prevention cloud server.

**detail**—(optional) Debug mode that provides more verbose output.

**pre-detection url**—(optional) Pre-detection mode where you can test your connection to the cloud server prior to actually enrolling your SRX Series device.

To use this option, in the Web UI, click **Devices** and then click **Enroll**. You will receive an ops script similar to this:

```
op url https://abc.def.junipersecurity.net/bootstrap/enroll/AaBbCc/DdEeFf.slax
```

Use the root URL from the ops script as the url for the pre-detection option. For example, using the above ops script run the command as:

```
request services advanced-anti-malware diagnostic pre-detection
abc.def.junipersecurity.net
```

**routing-instance**—(optional) Routing instance used during enrollment. Specifying this option lets you diagnose the data plane connection to the Juniper Sky ATP cloud server with a customized routing instance. If you add **routing-instance ?** to the command line and press Enter, a list of known routing instances is displayed.

### Additional Information

[Table 66 on page 231](#) lists the error conditions detected by this CLI command.

**Table 66: aamw-diagnostics Script Error Messages**

Error Message	Description
URL unreachable is detected, please make sure URL <i>url</i> port <i>port</i> is reachable.	Could not access the cloud server.
SSL profile <i>ssl profile name</i> is inconsistent between PFE and RE.	The SSL profile exists in the RE but does not exist in the PFE.
SSL profile <i>ssl profile name</i> is empty.	The SSL profile has neither trusted CA nor client certificate configured.
SSL local certificate <i>local certificate</i> is inconsistent between PFE and RE.	The SSL client certificate does not exist in PFE.

Table 66: aamw-diagnostics Script Error Messages (continued)

Error Message	Description
SSL CA <i>ca name</i> is inconsistent between PFE and RE.	The SSL CA exists in the RE but does not exist in the PFE.
DNS lookup failure is detected, please check your DNS configuration.	The IP address of the cloud server could not be found.  If this test fails, check to make sure your Internet connection is working properly and your DNS server is configured and has an entry for the cloud URL.
To-SKYATP connection through management interface is detected. Please make sure to-SKYATP connection is through packet forwarding plane.	The test detected that the Internet connection to the cloud server is through the management interface. This may result in your PFE connection to the cloud server failing.  To correct this, change the Internet connection to the cloud to be through the PFE and not the management interface.
Unable to get server time.	Could not retrieve the server time.
Time difference is too large between server and this device.	The difference between the server time and the local SRX Series device's time is more than a minute.  To correct this, ensure that the clock on the local SRX device is set correctly. Also, verify that you are using the correct NTP server.
Unable to perform IP path MTU check since ICMP service is down.	Unable to connect to the Juniper Sky ATP cloud server.
Required ICMP session not found.	Unable to establish an ICMP session with the specified URL. Check that you have specified a valid URL.

**Required Privilege Level**

View

## RELATED DOCUMENTATION

| [request services advanced-anti-malware data-connection](#) | 228

**List of Sample Output**

[request services advanced-anti-malware diagnostic on page 233](#)

[request services advanced-anti-malware diagnostic detail on page 233](#)

[request services advanced-anti-malware diagnostic pre-detection on page 233](#)

## Sample Output

### request services advanced-anti-malware diagnostic

```
user@host> request services advanced-anti-malware diagnostic abc.def.junipersecurity.net
```

```
Time check                : [OK]
DNS check                 : [OK]
SKYATP reachability check : [OK]
SKYATP ICMP service check : [OK]
Interface configuration check : [OK]
Outgoing interface MTU is default value
IP Path MTU check        : [OK]
IP Path MTU is 1472
SSL configuration consistent check : [OK]
```

### request services advanced-anti-malware diagnostic detail

```
user@host> request services advanced-anti-malware diagnostic abc.def.junipersecurity.net detail
```

```
Time check                : [OK]
  [INFO]    Try to get IP address for hostname abc.def.junipersecurity.net
DNS check                 : [OK]
  [INFO]    Try to test SKYATP server connectivity
SKYATP reachability check : [OK]
  [INFO]    Try ICMP service in SKYATP
SKYATP ICMP service check : [OK]
  [INFO]    To-SKYATP connection is using ge-0/0/3.0, according to route
Interface configuration check : [OK]
Outgoing interface MTU is default value
  [INFO]    Check IP MTU with length 1472
IP Path MTU check        : [OK]
IP Path MTU is 1472
SSL configuration consistent check : [OK]
```

### request services advanced-anti-malware diagnostic pre-detection

```
user@host> request services advanced-anti-malware diagnostic pre-detection abc.def.junipersecurity.net
```

```

Time check : [OK]
DNS check : [OK]
SKYATP reachability check : [OK]
SKYATP ICMP service check : [OK]
Interface configuration check : [OK]
Outgoing interface MTU is default value
IP Path MTU check : [OK]
IP Path MTU is 1472

```

## Troubleshooting Juniper Sky Advanced Threat Prevention: Checking the application-identification License

If you are using an SRX1500 Series device, you must have a valid **application-identification** license installed. Use the **show services application-identification version** CLI command to verify the applications packages have been installed. You must have version 2540 or later installed. For example:

```

user@host> show services application-identification version
Application package version: 2540

```

If you do not see the package or the package version is incorrect, use the **request services application-identification download** CLI command to download the latest application package for Junos OS application identification. For example:

```

user@host> request services application-identification download
Please use command "request services application-identification download status" to check status

```

Then use the **request services application-identification install** CLI command to install the downloaded application signature package.

```

user@host> request services application-identification install
Please use command "request services application-identification install status" to check status

```

Use the **show services application-identification application version** CLI command again to verify the applications packages is installed.



## Viewing Juniper Sky Advanced Threat Prevention System Log Messages

The Junos OS generates system log messages (also called syslog messages) to record events that occur on the SRX Series device. Each system log message identifies the process that generated the message and briefly describes the operation or error that occurred. Juniper Sky ATP logs are identified with a **SRX\_AAWM\_ACTION\_LOG** or **SRX AAMWD** entry.

The following example configures basic syslog settings.

```
set groups global system syslog user * any emergency
set groups global system syslog host log kernel info
set groups global system syslog host log any notice
set groups global system syslog host log pfe info
set groups global system syslog host log interactive-commands any
set groups global system syslog file messages kernel info
set groups global system syslog file messages any any
set groups global system syslog file messages authorization info
set groups global system syslog file messages pfe info
set groups global system syslog file messages archive world-readable
```

To view events in the CLI, enter the following command:

**show log**

### Example Log Message

```
<14> 1 2013-12-14T16:06:59.134Z pinarello RT_AAMW - SRX_AAMW_ACTION_LOG
[junos@xxx.x.x.x.28 http-host="www.mytest.com" file-category="executable"
action="BLOCK" verdict-number="8" verdict-source="cloud/blacklist/whitelist"
source-address="x.x.x.1" source-port="57116" destination-address="x.x.x.1"
destination-port="80" protocol-id="6" application="UNKNOWN"
nested-application="UNKNOWN" policy-name="argon_policy" username="user1"
session-id-32="50000002" source-zone-name="untrust" destination-zone-name="trust"]

http-host=www.mytest.com file-category=executable action=BLOCK verdict-number=8
verdict-source=cloud source-address=x.x.x.1 source-port=57116
destination-address=x.x.x.1 destination-port=80 protocol-id=6 application=UNKNOWN
nested-application=UNKNOWN policy-name=argon_policy username=user1
session-id-32=50000002 source-zone-name=untrust destination-zone-name=trust
```

## Configuring traceoptions

In most cases, policy logging of the traffic being permitted and denied is sufficient to verify what Juniper Sky ATP is doing with the SRX Series device data. However, in some cases you may need more information. In these instances, you can use traceoptions to monitor traffic flow into and out of the SRX Series device.

Using trace options are the equivalent of debugging tools. To debug packets as they traverse the SRX Series device, you need to configure **traceoptions** and flag **basic-datapath**. This will trace packets as they enter the SRX Series device until they exit, giving you details of the different actions the SRX Series device is taking along the way. Refer to [Debugging the Data Path](#) in the SRX Series documentation for details.

A minimum **traceoptions** configuration must include both a target **file** and a **flag**. The target **file** determines where the trace output is recorded. The **flag** defines what type of data is collected. For more information on using **traceoptions**, see the documentation for your SRX Series device.

To set the trace output file, use the **file filename** option. The following example defines the trace output file as **srx\_aamw.log**:

```
user@host# edit services advanced-anti-malware traceoptions
[edit services advanced-anti-malware traceoptions]
user@host# set file srx_aamw.log
```

where **flag** defines what data to collect and can be one of the following values:

- **all**—Trace everything.
- **connection**—Trace connections to the server.
- **content**—Trace the content buffer management.
- **daemon**—Trace the Juniper Sky ATP daemon.
- **identification**—Trace file identification.
- **parser**—Trace the protocol context parser.
- **plugin**—Trace the advanced anti-malware plugin.
- **policy**—Trace the advanced anti-malware policy.

The following example traces connections to the SRX device and the advanced anti-malware policy:

```
user@host# edit services advanced-anti-malware traceoptions
[edit services advanced-anti-malware traceoptions]
user@host# set services advanced-anti-malware traceoptions file skyatp.log
user@host# set services advanced-anti-malware traceoptions file size 100M
```

```
user@host# set services advanced-anti-malware traceoptions level all
user@host# set services advanced-anti-malware traceoptions flag all
```

Before committing your **traceoption** configuration, use the **show services advanced-anti-malware** command to review your settings.

```
# show services advanced-anti-malware
url https://xxx.xxx.xxx.com;
authentication {
    tls-profile
    ...
}
traceoptions {
    file skyatp.log;
    flag all;
    ...
}
...
```

You can also configure public key infrastructure (PKI) trace options. For example:

```
set security pki traceoptions file pki.log
set security pki traceoptions flag all
```

Debug tracing on both the Routing Engine and the Packet Forwarding Engine can be enabled for SSL proxy by setting the following configuration:

```
set services ssl traceoptions file ssl.log
set services ssl traceoptions file size 100m
set services ssl traceoptions flag all
```

You can enable logs in the SSL proxy profile to get to the root cause for the drop. The following errors are some of the most common:

- Server certification validation error.
- The trusted CA configuration does not match your configuration.
- System failures such as memory allocation failures.

- Ciphers do not match.
- SSL versions do not match.
- SSL options are not supported.
- Root CA has expired. You need to load a new root CA.

Set flow trace options to troubleshoot traffic flowing through your SRX Series device:

```
set security flow traceoptions flag all
set security flow traceoptions file flow.log size 100M
```

## RELATED DOCUMENTATION

[Enabling Debugging and Tracing for SSL Proxy traceoptions \(Security PKI\)](#)

## Viewing the traceoptions Log File

Once you commit the configuration, **traceoptions** starts populating the log file with data. Use the **show log** CLI command to view the log file. For example:

```
user@host> show log srx_aamw.log
```

Use **match**, **last** and **trim** commands to make the output more readable. For more information on using these commands, see [Configuring Traceoptions for Debugging and Trimming Output](#).

## Turning Off traceoptions

**traceoptions** is very resource-intensive. We recommend you turn off **traceoptions** when you are finished to avoid any performance impact. There are two ways to turn off **traceoptions**.

The first way is to use the **deactivate** command. This is a good option if you need to activate the trace in the future. Use the **activate** command to start capturing again.

```
user@host# deactivate services advanced-anti-malware traceoptions
user@host# commit
```

The second way is to remove **traceoptions** from the configuration file using the **delete** command.

```
user@host# delete services advanced-anti-malware traceoptions
user@host# commit
```

You can remove the **traceoptions** log file with the **file delete filename** CLI command or clear the contents of the file with the **clear log filename** CLI command.

## Juniper Sky Advanced Threat Prevention Dashboard Reports Not Displaying

Juniper Sky ATP dashboard reports require the Juniper Sky ATP premium license for the C&C Server & Malware report. If you do not see any data in this dashboard report, make sure that you have purchased a premium license.

**NOTE:** Juniper Sky ATP does not require you to install a license key onto your SRX Series device. Instead, your entitlement for a specific serial number is automatically transferred to the cloud server. It may take up to 24 hours for your activation to be updated in the Juniper Sky Advanced Threat cloud server. For more information, see *Obtaining the Juniper Sky Advanced Threat Prevention License*.

All reports are specific to your realm; no report currently covers trends derived from the Juniper Sky ATP worldwide database. Data reported from files uploaded from your SRX Series devices and other features make up the reports shown in your dashboard.

If you did purchase a premium license and followed the configuration steps ([Quick Start](#) or [“Juniper Sky Advanced Threat Prevention Configuration Overview” on page 31](#)) and are still not seeing data in the dashboard reports, contact Juniper Networks Technical Support.

## Juniper Sky Advanced Threat Prevention RMA Process

On occasion, because of hardware failure, a device needs to be returned for repair or replacement. For these cases, contact Juniper Networks, Inc. to obtain a Return Material Authorization (RMA) number and follow the [RMA Procedure](#).

Once you transfer your license keys to the new device, it may take up to 24 hours for the new serial number to be registered with the Juniper Sky ATP cloud service.



**WARNING:** After any serial number change on the SRX Series device, a new RMA serial number needs to be re-enrolled with Juniper Sky ATP cloud. This means that you must enroll your replacement unit as a new device. See [“Enrolling an SRX Series Device With Juniper Sky Advanced Threat Prevention” on page 43](#). Juniper Sky ATP does not have an “RMA state”, and does not see these as replacement devices from a configuration or registration point of view. Data is not automatically transferred to the replacement SRX Series device from the old device.

# 8

PART

## More Documentation

---

[Sky ATP Tech Library Page Links](#) | 242

---

# Sky ATP Tech Library Page Links

## IN THIS CHAPTER

- [Links to Documentation on Juniper.net](#) | 242

## Links to Documentation on Juniper.net

- For more information, visit the [Sky ATP page](#) in the Juniper Networks TechLibrary.
- For information on configuring the SRX Series with Sky ATP using the available CLI commands, refer to the [Sky Advanced Threat Prevention CLI Reference Guide](#).
- For troubleshooting information, refer to the [Sky Advanced Threat Prevention Troubleshooting Guide](#).
- For information on the SRX Series, visit the [SRX Series Services Gateways page](#) in the Juniper Networks TechLibrary.