

EXHIBIT 17



Sky ATP

Sky Advanced Threat Prevention Administration Guide



Modified: 2018-01-25

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. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Sky ATP Sky Advanced Threat Prevention Administration Guide
Copyright © 2018 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 <http://www.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	xi
	Documentation and Release Notes	xi
	Documentation Conventions	xi
	Documentation Feedback	xiii
	Requesting Technical Support	xiv
	Self-Help Online Tools and Resources	xiv
	Opening a Case with JTAC	xiv
Part 1	Overview and Installation	
Chapter 1	Sky Advanced Threat Prevention Overview	3
	Juniper Networks Sky Advanced Threat Prevention	3
	Sky ATP Features	4
	How the SRX Series Device Remediates Traffic	6
	Sky ATP Use Cases	7
	How is Malware Analyzed and Detected?	8
	Cache Lookup	9
	Antivirus Scan	9
	Static Analysis	10
	Dynamic Analysis	10
	Machine Learning Algorithm	10
	Threat Levels	11
	Sky Advanced Threat Prevention License Types	11
	Additional License Requirements	12
	About Policy Enforcer	13
Chapter 2	Install Sky Advanced Threat Prevention	15
	Sky Advanced Threat Prevention Installation Overview	15
	Managing the Sky Advanced Threat Prevention License	15
	Obtaining the Premium License Key	16
	License Management and SRX Series Devices	16
	Sky ATP Premium Evaluation License for vSRX	17
	License Management and vSRX Deployments	17
	High Availability	18
	Registering a Sky Advanced Threat Prevention Account	19
	Downloading and Running the Sky Advanced Threat Prevention Script	23

Part 2	The Web Portal and Enrolling SRX Series Devices	
Chapter 3	The Sky ATP Web Portal	31
	Sky Advanced Threat Prevention Configuration Overview	31
	Sky Advanced Threat Prevention Web UI Overview	33
	Accessing the Web UI	34
	Dashboard Overview	36
	Reset Password	37
Chapter 4	Enroll SRX Series Devices	39
	Enrolling an SRX Series Device With Sky Advanced Threat Prevention	39
	Removing an SRX Series Device From Sky Advanced Threat Prevention	41
	Searching for SRX Series Devices Within Sky Advanced Threat Prevention	42
	Sky Advanced Threat Prevention RMA Process	45
	Device Information	45
	Cloud Feeds for Sky Advanced Threat Prevention: More Information	46
Part 3	Configure	
Chapter 5	Whitelists and Blacklists	49
	Sky Advanced Threat Prevention Whitelist and Blacklist Overview	49
	Creating Whitelists and Blacklists	51
Chapter 6	Email Scanning: Sky ATP	53
	Email Management Overview	53
	SMTP Quarantine Overview: Blocked Emails	55
	Email Management: Configure SMTP	56
	IMAP Block Overview	59
	Email Management: Configure IMAP	60
	Email Management: Configure Blacklists and Whitelists	62
Chapter 7	Email Scanning: SRX Series Device	63
	Configuring the SMTP Email Management Policy on the SRX Series Device	63
	Configuring the IMAP Email Management Policy on the SRX Series Device	68
	Configuring Reverse Proxy on the SRX Series Device	74
Chapter 8	File Inspection Profiles	77
	File Inspection Profiles Overview	77
	Creating File Inspection Profiles	79
Chapter 9	External Threat Feeds	81
	Enabling External Threat Feeds	81
Chapter 10	Global Configurations	85
	Global Alert Configuration Overview	85
	Creating and Editing the Global Alert Configuration	85
	Configuring Threat Intelligence Sharing	86
	Configuring Trusted Proxy Servers	88

Part 4	Monitor and Take Action	
Chapter 11	Hosts	91
	Hosts Overview	91
	Host Details	93
Chapter 12	Identifying Infected Hosts	95
	Compromised Hosts: More Information	95
	About Block Drop and Block Close	99
	Host Details	99
	Configuring the SRX Series Devices to Block Infected Hosts	101
Chapter 13	Command and Control Servers	103
	Command and Control Servers Overview	103
	Command and Control Server Details	104
Chapter 14	Identify Hosts Communicating with Command and Control Servers	107
	Command and Control Servers: More Information	107
	Configuring the SRX Series Device to Block Outbound Requests to a C&C Host	109
Chapter 15	File Scanning	111
	HTTP File Download Overview	111
	HTTP File Download Details	112
	File Summary	113
	HTTP Downloads	114
	Sample STIX Report	115
	Manual Scanning Overview	115
	File Scanning Limits	116
Chapter 16	Email Scanning	119
	Email Attachments Scanning Overview	119
	Email Attachments Scanning Details	120
	File Summary	121
Part 5	Policies on the SRX Series Device	
Chapter 17	Configure Sky ATP Policies on the SRX Series Device	125
	Sky Advanced Threat Prevention Policy Overview	125
	Enabling Sky ATP for Encrypted HTTPS Connections	128
	Example: Configuring a Sky Advanced Threat Prevention Policy Using the CLI ..	129
Chapter 18	Configure IP-Based Geolocations on the SRX Series Device	133
	Geolocation IPs and Sky Advanced Threat Prevention	133
	Configuring Sky Advanced Threat Prevention With Geolocation IP	134
Part 6	Administration	
Chapter 19	Sky ATP Administration	139
	Modifying My Profile	139
	Creating and Editing User Profiles	140
	Application Tokens Overview	141

	Creating Application Tokens	141
Part 7	Troubleshoot	
Chapter 20	Troubleshooting Topics	145
	Sky Advanced Threat Prevention Troubleshooting Overview	145
	Troubleshooting Sky Advanced Threat Prevention: Checking DNS and Routing Configurations	146
	Troubleshooting Sky Advanced Threat Prevention: Checking Certificates	148
	Troubleshooting Sky Advanced Threat Prevention: Checking the Routing Engine Status	149
	request services advanced-anti-malware data-connection	151
	request services advanced-anti-malware diagnostic	153
	Troubleshooting Sky Advanced Threat Prevention: Checking the application-identification License	156
	Viewing Sky Advanced Threat Prevention System Log Messages	156
	Configuring traceoptions	157
	Viewing the traceoptions Log File	159
	Turning Off traceoptions	159
	Sky Advanced Threat Prevention Dashboard Reports Not Displaying	160
	Sky Advanced Threat Prevention RMA Process	160
Part 8	More Documentation	
Chapter 21	Sky ATP Tech Library Page Links	165
	Links to Documentation on Juniper.net	165

List of Figures

Part 1	Overview and Installation	
Chapter 1	Sky Advanced Threat Prevention Overview	3
	Figure 1: Sky ATP Overview	3
	Figure 2: Sky ATP Components	5
	Figure 3: Inspecting Inbound Files for Malware	7
	Figure 4: Sky ATP Use Cases	8
	Figure 5: Example Sky ATP Pipeline Approach for Analyzing Malware	9
	Figure 6: Comparing Traditional SRX Customers to Policy Enforcer Customers	14
Chapter 2	Install Sky Advanced Threat Prevention	15
	Figure 7: Sky ATP Login	19
	Figure 8: Creating Your Sky ATP Realm Name	20
	Figure 9: Entering Your Sky ATP Contact Information	21
	Figure 10: Creating Your Sky ATP Credentials	22
	Figure 11: Enrolling Your SRX Series Device	24
	Figure 12: Example Enrolled SRX Series Device	25
Part 2	The Web Portal and Enrolling SRX Series Devices	
Chapter 3	The Sky ATP Web Portal	31
	Figure 13: Web UI Infotip	34
	Figure 14: Sky ATP Web UI Login Page	35
	Figure 15: Logging Out of the Management Interface	35
Chapter 4	Enroll SRX Series Devices	39
	Figure 16: Searching for a Device in the Web UI	43
	Figure 17: Example Device Search Results	44
Part 3	Configure	
Chapter 5	Whitelists and Blacklists	49
	Figure 18: Example Sky ATP Whitelist	50
Chapter 6	Email Scanning: Sky ATP	53
	Figure 19: Email Management Overview	54
Part 4	Monitor and Take Action	
Chapter 12	Identifying Infected Hosts	95
	Figure 20: Infected Host from Malware	96
	Figure 21: Viewing Infected Hosts	97

Chapter 15	File Scanning	111
	Figure 22: Sample STIX Report	115

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xii
	Table 2: Text and Syntax Conventions	xii
Part 1	Overview and Installation	
Chapter 1	Sky Advanced Threat Prevention Overview	3
	Table 3: Sky ATP Components	5
	Table 4: Threat Level Definitions	11
	Table 5: Comparing the Sky ATP Free Model, Basic-Threat Feed, and Premium Model	12
Part 2	The Web Portal and Enrolling SRX Series Devices	
Chapter 3	The Sky ATP Web Portal	31
	Table 6: Configuring Sky ATP	31
	Table 7: Sky ATP Dashboard Widgets	36
Chapter 4	Enroll SRX Series Devices	39
	Table 8: Button Actions	40
	Table 9: Device Information Fields	45
Part 3	Configure	
Chapter 6	Email Scanning: Sky ATP	53
	Table 10: Blocked Email Summary View	55
	Table 11: Blocked Email Detail View	55
	Table 12: Configure Quarantine Malicious Messages	57
	Table 13: Configure Deliver with Warning Headers	58
	Table 14: Permit	58
	Table 15: Blocked Email Summary View	59
	Table 16: Blocked Email Detail View	59
	Table 17: Configure Block Malicious Messages	60
Chapter 7	Email Scanning: SRX Series Device	63
	Table 18: Comparing Reverse Proxy Before and After Junos OS Release 15.1X49-D80	74
	Table 19: Supported SSL Proxy Configurations	75
Chapter 8	File Inspection Profiles	77
	Table 20: File Category Contents	77
	Table 21: Device Profile Settings	79

Chapter 10	Global Configurations	85
	Table 22: Global Configuration Fields	86
	Table 23: Additional Information	87
Part 4	Monitor and Take Action	
Chapter 11	Hosts	91
	Table 24: Operations for Multiple Infected Hosts	91
	Table 25: Compromised Host Information	92
	Table 26: Threat Level Recommendations	93
Chapter 13	Command and Control Servers	103
	Table 27: Command & Control Server Data Fields	104
	Table 28: Command & Control Server Contacted Host Data	105
	Table 29: Command & Control Server Associated Domains Data	105
	Table 30: Command & Control Server Signature Data	105
Chapter 15	File Scanning	111
	Table 31: HTTP Scanning Data Fields	111
	Table 32: Links on the HTTP File Download Details Page	112
	Table 33: General Summary Fields	113
	Table 34: File Scanning Data Fields	116
Chapter 16	Email Scanning	119
	Table 35: Email Attachments Scanning Data Fields	119
	Table 36: General Summary Fields	121
Part 5	Policies on the SRX Series Device	
Chapter 17	Configure Sky ATP Policies on the SRX Series Device	125
	Table 37: Sky ATP Security Policy Additions	126
Part 6	Administration	
Chapter 19	Sky ATP Administration	139
	Table 38: My Profile Fields	139
	Table 39: User Fields	140
	Table 40: Application Token Settings	142
Part 7	Troubleshoot	
Chapter 20	Troubleshooting Topics	145
	Table 41: Troubleshooting Sky ATP	146
	Table 42: Data Connection Test Output	151
	Table 43: aamw-diagnostics Script Error Messages	154

About the Documentation

- Documentation and Release Notes on page xi
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiv

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 <http://www.juniper.net/techpubs/>.

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 <http://www.juniper.net/books>.

Documentation Conventions

Table 1 on page xli 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 xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

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

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

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i> >;
(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.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
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		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <http://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Overview and Installation

- Sky Advanced Threat Prevention Overview on page 3
- Install Sky Advanced Threat Prevention on page 15

CHAPTER 1

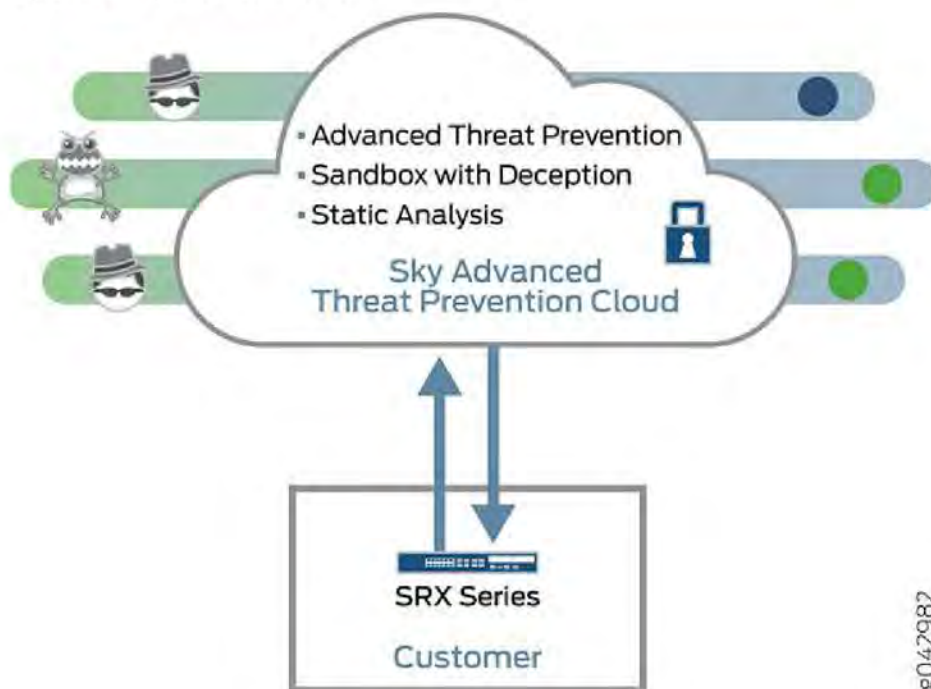
Sky Advanced Threat Prevention Overview

- Juniper Networks Sky Advanced Threat Prevention on page 3
- How is Malware Analyzed and Detected? on page 8
- Sky Advanced Threat Prevention License Types on page 11
- About Policy Enforcer on page 13

Juniper Networks Sky Advanced Threat Prevention

Juniper Networks Sky Advanced Threat Prevention (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: Sky ATP Overview



8042982

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.

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](#).

Sky ATP Features

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, 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 Sky ATP components.

Figure 2: Sky ATP Components

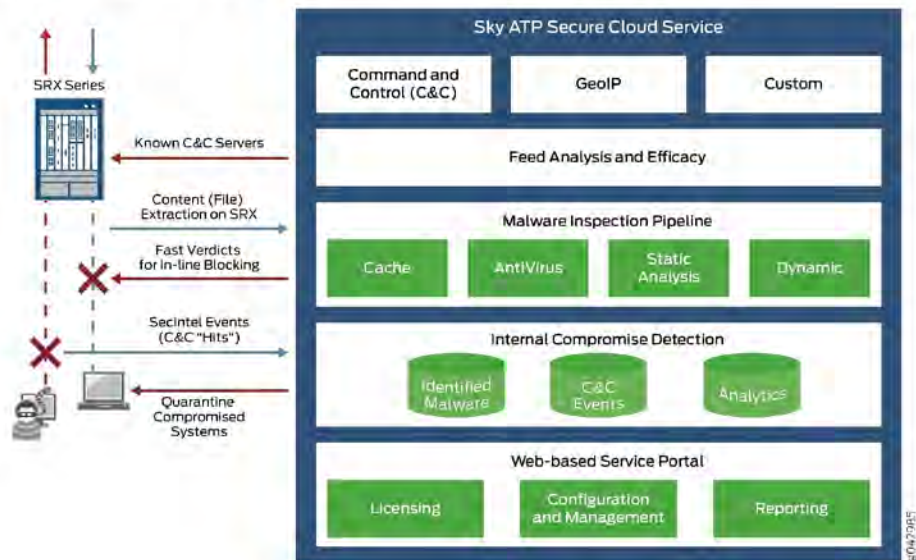


Table 3 on page 5 briefly describes each Sky ATP component's operation.

Table 3: 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.
GeoIP cloud feeds	GeoIP 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. NOTE: Custom feeds are not supported in this release.
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.

Table 3: Sky ATP Components (continued)

Component	Operation
Internal compromise detection	Inspects files, metadata, and other information.
Service portal (Web UI)	<p>Graphics interface displaying information about detected threats inside the customer network.</p> <p>Configuration management tool where customers can fine-tune which file categories can be submitted into the cloud for processing.</p>

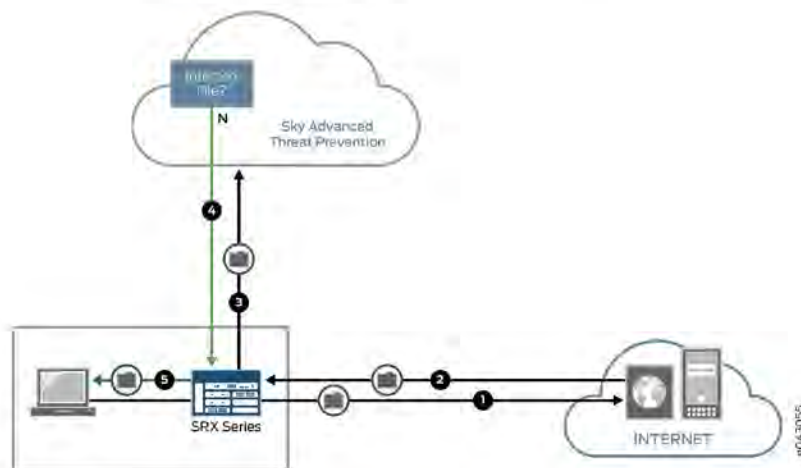
How the SRX Series Device Remediates Traffic

The SRX Series devices use intelligence provided by 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 Sky ATP cloud for inspection. The SRX Series device holds the last few KB of the file from the destination client while 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 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 8.

Figure 3 on page 7 shows an example flow of a client requesting a file download with Sky ATP.

Figure 3: Inspecting Inbound Files for Malware



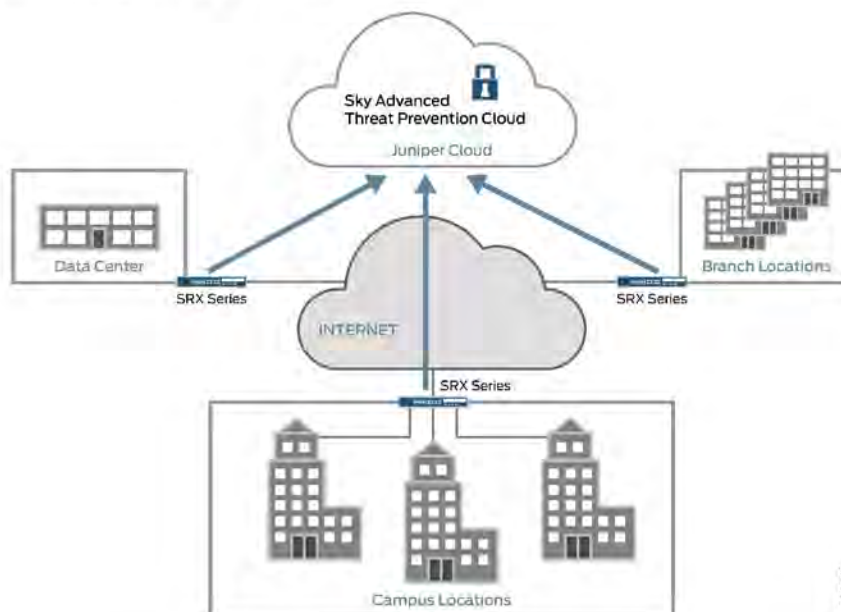
Step	Description
1	A client system behind an SRX Series devices requests a file download from the Internet. The SRX Series device forwards that request to the appropriate server.
2	The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must 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	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 Sky ATP. A list of infected hosts is available so that the SRX Series device can block inbound and outbound traffic.

Sky ATP Use Cases

Sky ATP can be used anywhere in an SRX Series deployment. See Figure 4 on page 8.

Figure 4: Sky ATP Use Cases



- Campus edge firewall—Sky ATP analyzes files downloaded from the Internet and protects end-user devices.
- Data center edge—Like the campus edge firewall, Sky ATP prevents infected files and application malware from running on your computers.
- Branch router—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.

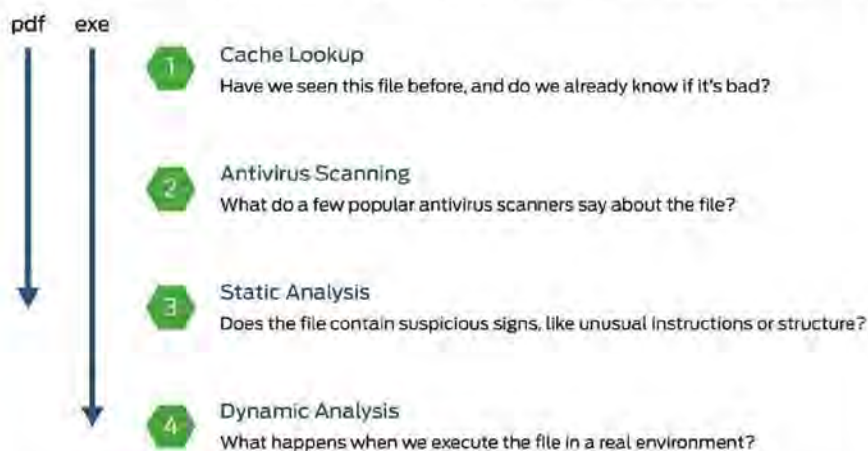
Related Documentation

- Sky Advanced Threat Prevention License Types on page 11

How is Malware Analyzed and Detected?

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 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 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 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 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.

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. Sky ATP uses a number of *deception techniques* to trick the malware into determining this is a real user environment. For example, 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 boosts 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

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

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.
7-10	High threat level.

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

Related Documentation

- [Juniper Networks Sky Advanced Threat Prevention on page 3](#)
- [Dashboard Overview on page 36](#)
- [Sky Advanced Threat Prevention License Types on page 11](#)

Sky Advanced Threat Prevention License Types

Sky ATP has three service levels:

- **Free**—The free model solution is available on all supported SRX Series devices (see the [Supported Platforms Guide](#)) and for customers that have a valid support contract, but only scans executable file types (see [Sky Advanced Threat Prevention Profile Overview](#)). Based on this result, the SRX Series device can allow the traffic or perform inline blocking.
- **Basic**—Includes executable file scanning and adds filtering using the following threat feed types: Command and Control, GeoIP, Custom Filtering, and Threat Intel feeds. Threat Intel feeds use APIs that allow you to inject feeds into Sky ATP.
- **Premium**—Includes all features provided in the Free and Basic licenses, but provides deeper analysis. All supported file types are scanned and examined using several analysis techniques to give better coverage. Full reporting provides details about the threats found on your network.



NOTE: You do not need to download any additional software to run Sky ATP.

[Table 5](#) on page 12 shows a comparison between the free model and the premium model.

Table 5: Comparing the Sky ATP Free Model, Basic-Threat Feed, and Premium Model

Free Model	Basic-Threat Feeds Model	Premium Model
Management through cloud interface. Zero-on premise footprint beyond the SRX Series device.	Management through cloud interface. Zero-on premise footprint beyond the SRX Series device.	Management through cloud interface. Zero-on premise footprint beyond the SRX Series device.
Inbound protection.	Inbound protection.	Inbound protection.
Outbound protection.	Outbound protection.	Outbound protection.
—	C&C feeds.	C&C feeds.
—	GeolP filtering.	GeolP filtering.
	Custom feeds	Custom feeds
		Infected host feed/endpoint quarantine
	Threat Intelligence APIs only	All APIs including File/Hash
—	—	C&C protection with event data returned to the Sky ATP cloud.
—	—	Compromised endpoint dashboard.
Inspects only executable file types. Executables go through the entire pipeline (cache, antivirus, static and dynamic).	Inspects only executable file types. Executables go through the entire pipeline (cache, antivirus, static and dynamic).	No restrictions on object file types inspected beyond those imposed by the Sky ATP service. You can specify which file types are sent to service for inspection.
Reporting with rich detail on malware behaviors.	Reporting with rich detail on malware behaviors.	Reporting with rich detail on malware behaviors.

For more information on analysis techniques, see "How is Malware Analyzed and Detected?" on page 8. For additional information on product options, see the Sky ATP datasheet.

For more information on this and premium license SKUs, contact your local sales representative.

Additional License Requirements

In addition to the Sky ATP license, you must have the following licenses installed on your devices for Sky ATP to work correctly:

- SRX340 and SRX345 Series devices—Purchase the JSE bundle (which includes AppSecure), or purchase the JSB bundle and the AppSecure license separately.
- SRX 550m Series devices—Purchase a bundle that includes AppSecure, or purchase the AppSecure license separately.
- SRX 1500 Series devices—Purchase the JSE bundle (which includes AppSecure.)
- SRX 5000 Series devices—Purchase a bundle that includes AppSecure, or purchase the AppSecure license separately.
- vSRX—Purchase a bundle that includes AppSecure, or purchase the AppSecure license separately.

About 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.

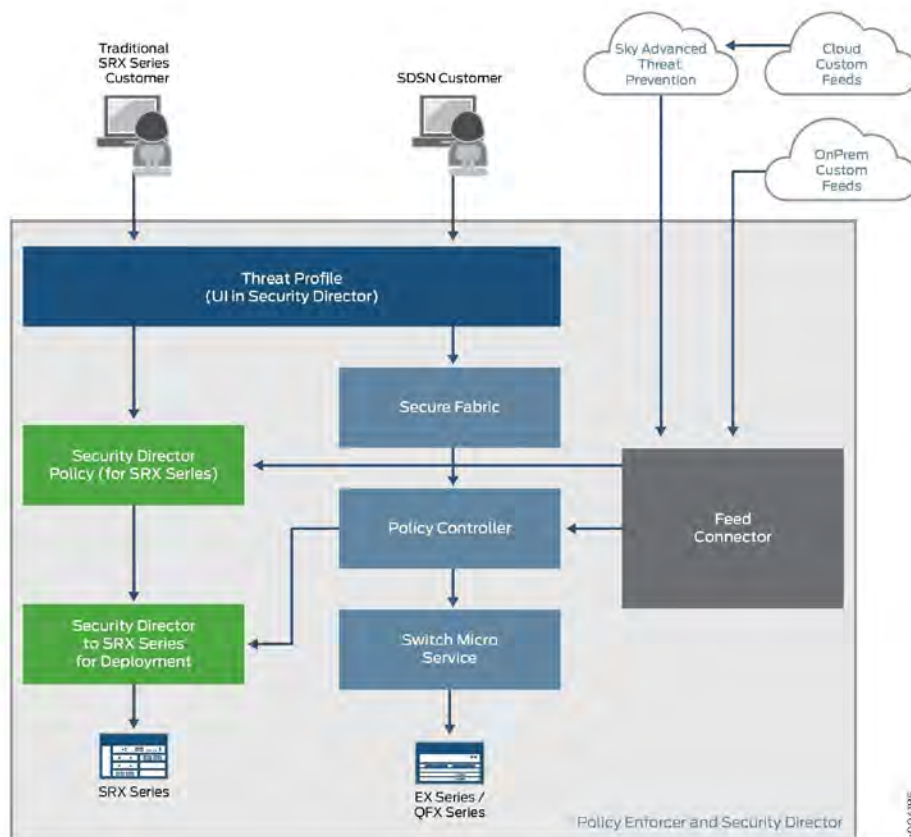
It also automates the enforcement of security policies across the network and quarantines infected endpoints to prevent threats across firewalls and switches. It works with cloud-based Sky Advanced Threat Prevention (Sky ATP) to protect both perimeter-oriented threats as well as threats within the network. 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 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 on page 91
- Host Details on page 93
- Dashboard Overview on page 36

CHAPTER 2

Install Sky Advanced Threat Prevention

- Sky Advanced Threat Prevention Installation Overview on page 15
- Managing the Sky Advanced Threat Prevention License on page 15
- Registering a Sky Advanced Threat Prevention Account on page 19
- Downloading and Running the Sky Advanced Threat Prevention Script on page 23

Sky Advanced Threat Prevention Installation Overview

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

1. (Optional) Obtain a Sky ATP premium license. See *Obtaining the Sky Advanced Threat Prevention License*.
2. Register an account on the Sky ATP cloud Web portal. See "Registering a Sky Advanced Threat Prevention Account" on page 19.
3. Download and run the Sky ATP script on your SRX Series device. See "Downloading and Running the Sky Advanced Threat Prevention Script" on page 23.

The following sections describe these steps in more detail.

Managing the Sky Advanced Threat Prevention License

This topic describes how to install the Sky ATP premium license onto your SRX Series devices and vSRX deployments. You do not need to install the Sky ATP free license as these are included your base software. Note that the free license has a limited feature set (see *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 Sky ATP premium license available for the SRX Series device cannot be used on vSRX deployments.

- Obtaining the Premium License Key on page 16
- License Management and SRX Series Devices on page 16

- Sky ATP Premium Evaluation License for vSRX on page 17
- License Management and vSRX Deployments on page 17
- High Availability on page 18

Obtaining the Premium License Key

The 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 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 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
FPC 0         REV 08   711-053832   ACMG3280      FEB
PIC 0         BUILTIN  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://www.juniper.net/generate_license/.
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, 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 Sky ATP cloud server.

Sky ATP Premium Evaluation License for vSRX

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

Instructions for downloading the trial license are here:
<http://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 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 Sky ATP. For more information, see [Registering a Sky Advanced Threat Prevention Account](#).

License Management and vSRX Deployments

Unlike with physical SRX Series devices, you must install Sky ATP premium licenses onto your vSRX. Installing the 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 Sky ATP license key on your vSRX, you must first remove the existing 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.

You can install the license key on as many vSRX deployments as needed. However, be aware that this can affect your file limitation. For example, suppose you purchased a premium license that has a 10,000 files per day submission to cloud limit. If you install the premium license on 1000 vSRX deployments and each deployment submits 10 files to the cloud within the first hour of a day, then no more submissions can be made for the remainder of that day.

High Availability

Before enrolling your devices with the 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 Sky ATP cloud will recognize this is an HA cluster and will automatically enroll the other node.

Registering a Sky Advanced Threat Prevention Account

To create a 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 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.

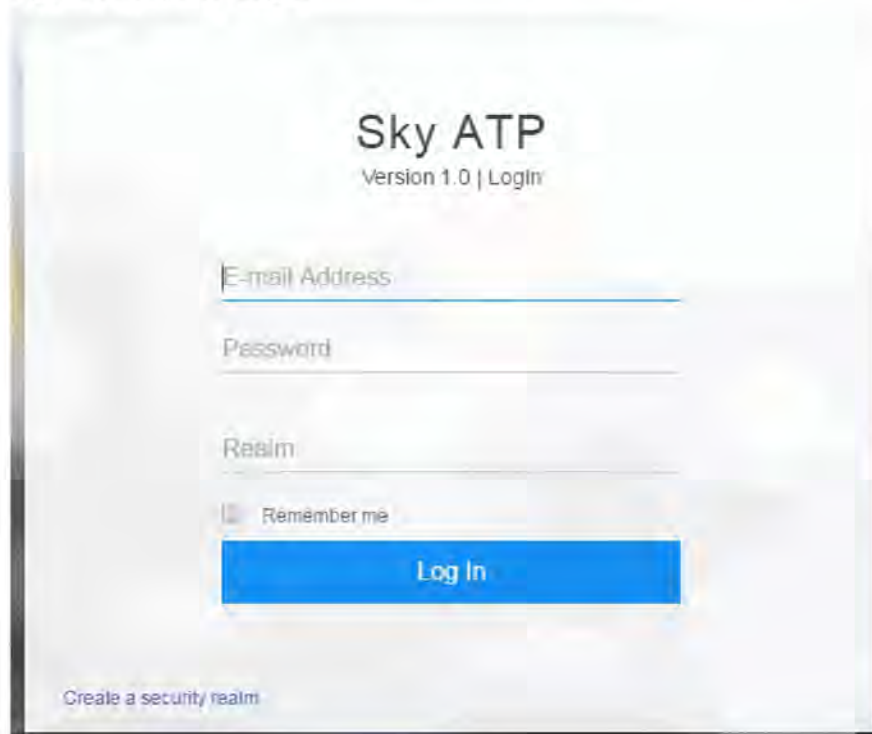
To create a Sky ATP administrator account:

1. Open a Web browser, type the following URL and press **Enter**.

<https://sky.junipersecurity.net>

The management interface login page appears. See [Figure 7](#) on page 19.

Figure 7: Sky ATP Login



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

The authentication window appears. See [Figure 8](#) on page 20.

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 20.

Figure 8: Creating Your Sky ATP Realm Name

Sky ATP ?

1 Realm Info 2 Contact Info 3 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

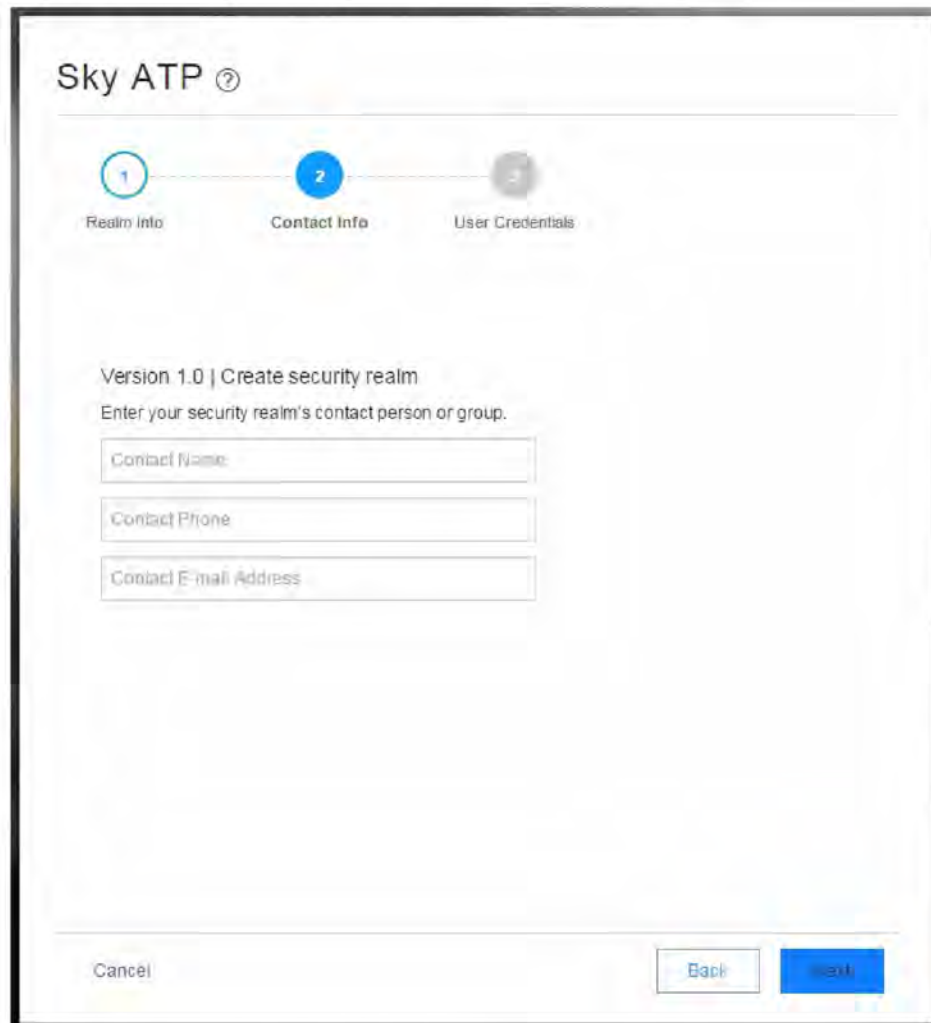
4. Enter your unique realm name, company name, and optionally a description. Then press **Next**.



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 21.

Figure 9: Entering Your Sky ATP Contact Information



The screenshot shows a web interface for 'Sky ATP' with a progress indicator at the top showing three steps: '1 Realm Info', '2 Contact Info' (the current step), and '3 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, 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 22.

Figure 10: Creating Your 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 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.

Downloading and Running the Sky Advanced Threat Prevention Script

The Sky ATP uses a Junos OS operation (op) script to help you configure your SRX Series device to connect to the 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 Sky ATP configuration on the SRX Series device.
- Establishes a secure connection to the cloud server.



NOTE: 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.

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 before running the op script or before running the **set services advanced-anti-malware connection** command. A reboot of your SRX Series device is required if you are using C&C or GeolP feeds.

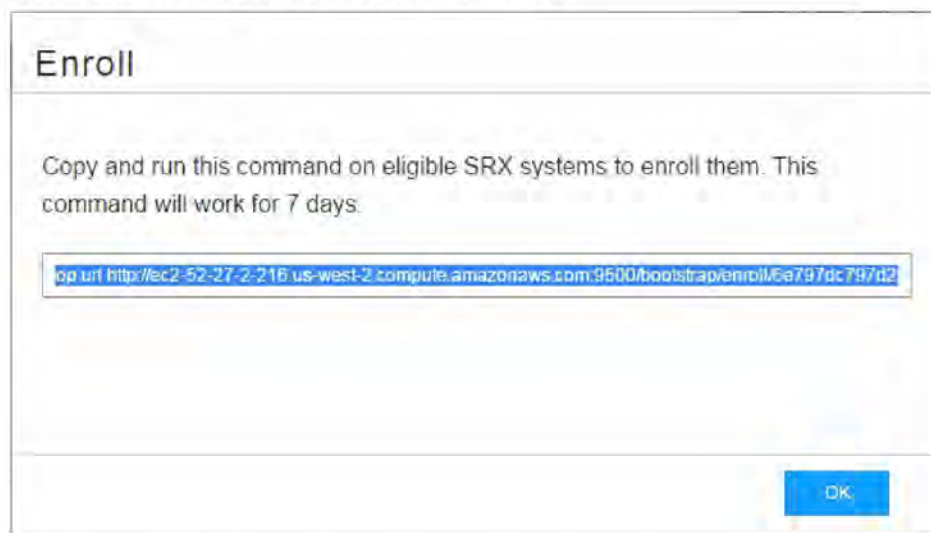
```
user@host> set security forwarding-process enhanced-services-mode
```


To download and run the Sky ATP script:

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

The Enroll window appears. See Figure 11 on page 24.

Figure 11: Enrolling Your SRX Series Device



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



NOTE: When enrolling devices, 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 Sky ATP and press **Enter**. Your screen will look similar to the following.

```
root@mysystem> op url http://skyatp.argon.junipersecurity.net/bootstrap/
enroll/6e797dc797d26129dae46f17a7255650/jpz1qkddod1cav5g.s1ax
Version JUNOS Software Release [15.1-X49] is valid for bootstrapping.
Going to enroll single device for SRX1500: PIC_00000067 with hostname
mysystem..
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 Sky Advanced Threat Prevention*) and then re-enroll it.

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

The SRX Series device you enrolled now appears in the table. See [Figure 12 on page 25](#).

Figure 12: Example Enrolled SRX Series Device

Device ID	Hostname	IP Address	License	Last Enrolling Attempt	Last Update
0A024A40001	pev-fdge01	192.168.1.100	premium	Jan 23, 2016 9:03 AM	Jan 23, 2016 9:03 AM
0A0311A0002	pev-cgpr01	192.168.1.101	premium	Jan 23, 2016 9:12 AM	Jan 23, 2016 9:12 AM

- (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 Sky ATP configuration on the SRX Series device. These include:



NOTE: You do not need to 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 setting is determined by your geographical region.

```
set services advanced-anti-malware connection url
https://skyatp.argon.junipersecurity.net
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.argon.junipersecurity.net/
api/manifest.xml
set services security-intelligence authentication tls-profile aamw-ssl
```

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
```

To check your certificates, see "Troubleshooting Sky Advanced Threat Prevention: Checking Certificates" on page 148. We recommend that you re-run the op script if you are having certificate issues.

PART 2

The Web Portal and Enrolling SRX Series Devices

- The Sky ATP Web Portal on page 31
- Enroll SRX Series Devices on page 39

CHAPTER 3

The Sky ATP Web Portal

- Sky Advanced Threat Prevention Configuration Overview on page 31
- Sky Advanced Threat Prevention Web UI Overview on page 33
- Dashboard Overview on page 36
- Reset Password on page 37

Sky Advanced Threat Prevention Configuration Overview

Table 6 on page 31 lists the basic steps to configure Sky ATP.



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

Table 6: Configuring 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>
Enroll your SRX Series devices	Select the SRX Series devices to communicate with Sky ATP. Only those listed in the management interface can send files to the cloud for inspection and receive results. This step is done in the Web UI and on your SRX Series device.	"Enrolling an SRX Series Device With Sky Advanced Threat Prevention" on page 39
Set global configurations	Select Configure > Global Configuration 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.	Web UI tooltips and online help

Table 6: Configuring Sky ATP (*continued*)

Task	Description	For information, see
(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>	"Sky Advanced Threat Prevention Whitelist and Blacklist Overview" on page 49
(optional) Create the Sky ATP profile	<p>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>	<i>Sky Advanced Threat Prevention Profile Overview</i>
(optional) Identify compromised hosts	<p>Compromised hosts are systems where there is a high confidence that attackers have gained unauthorized access. Once identified, 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>	"Compromised Hosts: More Information" on page 95
(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&C server on the Internet.</p> <p>This step is done on the SRX Series device.</p> <p>NOTE: Requires Sky ATP premium license.</p>	"Command and Control Servers: More Information" on page 107
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>	"Sky Advanced Threat Prevention Policy Overview" on page 125
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&C server.</p> <p>This step is done on the SRX Series device.</p>	<p>"Configuring the SRX Series Devices to Block Infected Hosts" on page 101</p> <p>"Configuring the SRX Series Device to Block Outbound Requests to a C&C Host" on page 109</p>

Table 6: Configuring Sky ATP (*continued*)

Task	Description	For information, see
Enable the firewall policy	Create your SRX Series firewall policy to filter and log traffic in the network using the set security policies from-zone to-zone CLI commands. This step is done on the SRX Series device.	"Configuring the SRX Series Devices to Block Infected Hosts" on page 101 "Configuring the SRX Series Device to Block Outbound Requests to a C&C Host" on page 109 "Example: Configuring a Sky Advanced Threat Prevention Policy Using the CLI" on page 129

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 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.

Sky Advanced Threat Prevention Web UI Overview

The 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 Sky ATP. For more information using Security Director with Sky ATP, see the *Policy Enforcer administration guide* and the Security Director online help. The remainder of this guide refers to using 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 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 Figure 13 on page 34.

Figure 13: Web UI Infotip



Accessing the Web UI

To access the Sky ATP Web UI:

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

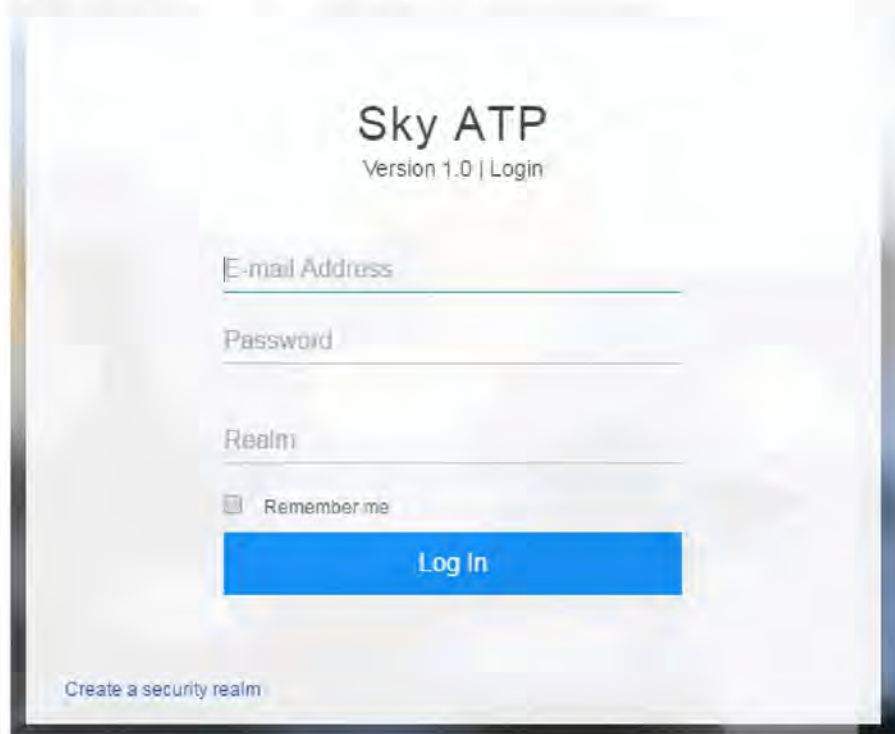
For information on supported browsers and their version numbers, see the *Sky Advanced Threat Prevention Supported Platforms Guide*.

2. Type the following URL and press Enter.

`https://sky.junipersecurity.net`

The Web UI login page appears. See Figure 14 on page 35.

Figure 14: Sky ATP Web UI Login Page



Sky ATP
Version 1.0 | Login

E-mail Address

Password

Realm

Remember me

Log In

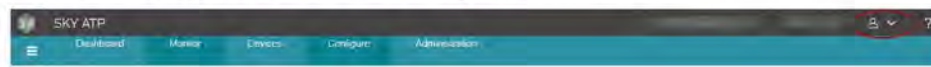
Create a security realm

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.

To terminate your session at any time, click the icon in the upper-right corner and click **Logout**. See Figure 15 on page 35.

Figure 15: Logging Out of the Management Interface



Dashboard Overview

The 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 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 GeoIP filtering feeds are only available with the Basic-Threat Feed or Premium license. For information on other licensed features, see *Sky Advanced Threat Prevention License Types*.

Available dashboard widgets are as follows:

Table 7: 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.
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 on page 37](#)
- [Juniper Networks Sky Advanced Threat Prevention on page 3](#)
- [How Is Malware Analyzed and Detected? on page 8](#)
- [Hosts Overview on page 91](#)
- [HTTP File Download Overview on page 111](#)
- [Command and Control Servers Overview on page 103](#)

Reset Password

If you forget your password to login to the Sky ATP dashboard, you can reset it using a link sent by email when you click **Forgot Password** from the 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 139 for those instructions.

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

1. Click the **Forgot Password** link on the 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 on page 139](#)
- [Creating and Editing User Profiles on page 140](#)

- [Dashboard Overview on page 36](#)

CHAPTER 4

Enroll SRX Series Devices

- Enrolling an SRX Series Device With Sky Advanced Threat Prevention on page 39
- Removing an SRX Series Device From Sky Advanced Threat Prevention on page 41
- Searching for SRX Series Devices Within Sky Advanced Threat Prevention on page 42
- Sky Advanced Threat Prevention RMA Process on page 45
- Device Information on page 45
- Cloud Feeds for Sky Advanced Threat Prevention: More Information on page 46

Enrolling an SRX Series Device With Sky Advanced Threat Prevention

Only devices enrolled with 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 Sky Advanced Threat Prevention” on page 42). 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.

Sky ATP uses a Junos OS operation (op) script to help you configure your SRX Series device to connect to the 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 Sky ATP configuration on the SRX Series device.
- Establishes a secure connection to the cloud server.



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

To enroll a device in Sky ATP, 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 Sky ATP and press **Enter**.



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 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 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 8: Button Actions

Threat Level	Definition
Enroll	Use the Enroll button to obtain a enroll command to run on eligible SRX Series devices. This command enrolls them in 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 Sky ATP. This command removes those devices from Sky ATP enrollment and is valid for 7 days.
Device Lookup	Use the Device Lookup button 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 Sky ATP.

Table 8: Button Actions (*continued*)

Threat Level	Definition
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: 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.

Related Documentation

- Sky Advanced Threat Prevention RMA Process on page 45
- Removing an SRX Series Device From Sky Advanced Threat Prevention on page 41
- Searching for SRX Series Devices Within Sky Advanced Threat Prevention on page 42
- Device Information on page 45

Removing an SRX Series Device From 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 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 Sky Advanced Threat Prevention on page 42
- Enrolling an SRX Series Device With Sky Advanced Threat Prevention on page 39
- Device Information on page 45

Searching for SRX Series Devices Within Sky Advanced Threat Prevention

You can search for any SRX Series device enrolled within your security realm of Sky Advanced Threat Prevention using the Device Lookup option. This option is another way for you to view if the device is using the free license or the premium license.



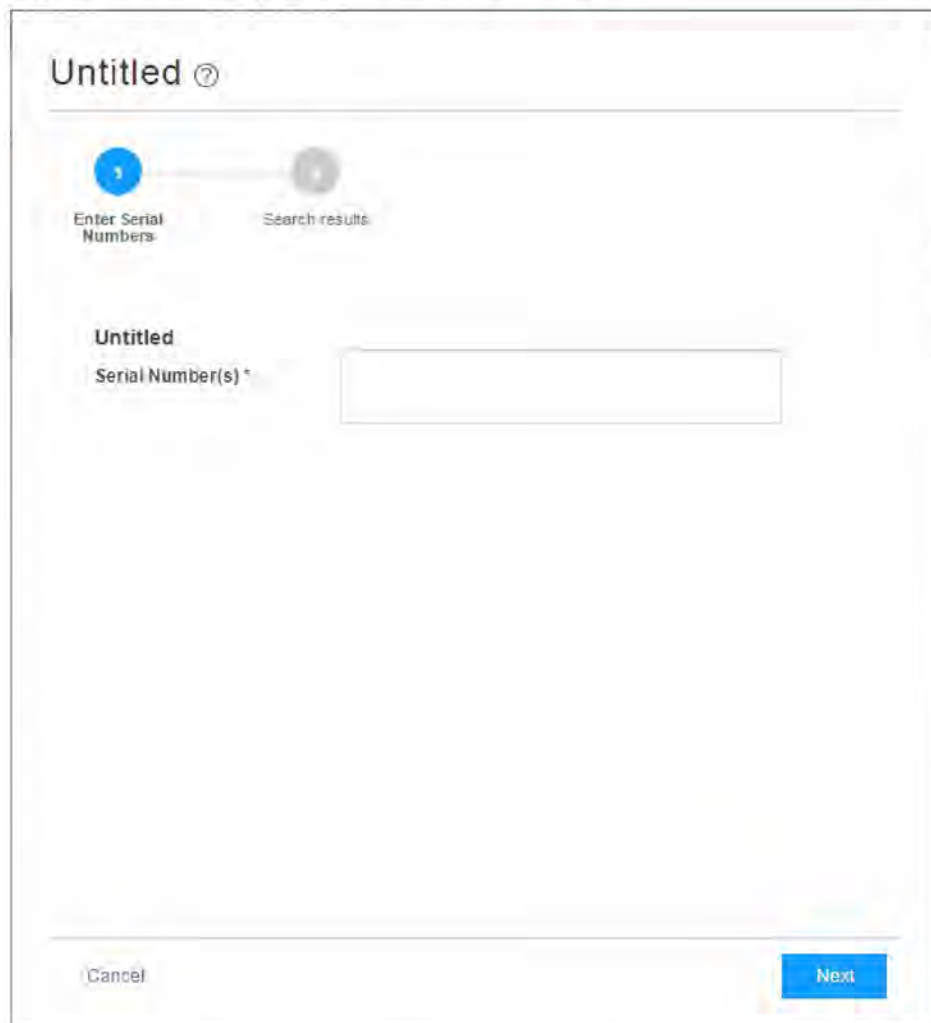
NOTE: With this release, you can only search for device using serial numbers.

To search for devices enrolled with Sky Advanced Threat Prevention:

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

The Device Lookup window appears. See Figure 16 on page 43.

Figure 16: Searching for a Device in the Web UI



The screenshot shows a web interface window titled "Untitled". At the top, there is a progress indicator with two steps: "Enter Serial Numbers" (highlighted with a blue circle and a question mark) and "Search results" (greyed out). Below this, the text "Untitled" is followed by a label "Serial Number(s) *" and a large empty text input field. At the bottom of the window, 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 17 on page 44.

Figure 17: Example Device Search Results

Untitled ?

1 Enter Serial Numbers 2 Search results

Untitled

Serial Number	Model Number	Tier
UKLG0YN0OADI	SRX100	free
UVPTES0UEC4D	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 on page 45
- Enrolling an SRX Series Device With Sky Advanced Threat Prevention on page 39
- Removing an SRX Series Device From Sky Advanced Threat Prevention on page 41
- Searching for SRX Series Devices Within Sky Advanced Threat Prevention on page 42

Sky Advanced Threat Prevention RMA Process

Sometimes, 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 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 Sky ATP cloud. This means that you must enroll your replacement unit as a new device. See “Enrolling an SRX Series Device With Sky Advanced Threat Prevention” on page 39. 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 9: 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 Sky ATP or if it has reached its daily limit. (At this time, the limit is 10,000 files per day for premium accounts.)
Configuration Information	
Up to date or Out of sync	This field indicates whether the Sky ATP configuration (whitelists, blacklists, global configuration, profile configuration) is in sync with the cloud configuration. If not, you can sync it here.
Connection Type	

Table 9: Device Information Fields (*continued*)

Field	Definition
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 Sky Advanced Threat Prevention on page 39
 - Removing an SRX Series Device From Sky Advanced Threat Prevention on page 41
 - Searching for SRX Series Devices Within Sky Advanced Threat Prevention on page 42

Cloud Feeds for 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 Sky Advanced Threat Prevention Script" on page 23. 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.argon.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.

PART 3

Configure

- Whitelists and Blacklists on page 49
- Email Scanning: Sky ATP on page 53
- Email Scanning: SRX Series Device on page 63
- File Inspection Profiles on page 77
- External Threat Feeds on page 81
- Global Configurations on page 85

CHAPTER 5

Whitelists and Blacklists

- Sky Advanced Threat Prevention Whitelist and Blacklist Overview on page 49
- Creating Whitelists and Blacklists on page 51

Sky Advanced Threat Prevention Whitelist and Blacklist Overview

A whitelist contains known trusted IP 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.

There are four kinds of whitelists and blacklists. Each list has Global items added and updated by the cloud. There are also Custom lists that allow you to add items manually. All are configured on the Sky ATP cloud server. The priority order is as follows:

- Custom whitelist
- Custom blacklist
- Global whitelist
- Global blacklist

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



NOTE: The global whitelist and global blacklist contents are hidden. You cannot view or edit them.

Whitelists and blacklists support the following types:

- URL
- IP address
- Hostname

The Web UI performs basic syntax checks to ensure your entries are valid.

Figure 18 on page 50 shows an example whitelist.

Figure 18: Example Sky ATP Whitelist



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 Sky Advanced Threat Prevention Script" on page 23.

Sky ATP periodically polls for new and updated content and automatically downloads them 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` 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 Output

```
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     global_whitelist ID-00000003
2        x.x.0.0       x.x.0.10     global_blacklist ID-00000004
```

If you do not see your updates, wait a few minutes and try the command again. You might be outside the 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 `aamwpolicy1` and creates log entries.

```
set services advanced-anti-malware policy aamwpolicy1 blacklist-notification log
set services advanced-anti-malware policy aamwpolicy1 whitelist-notification log
```

Creating Whitelists and Blacklists

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

Use the whitelist and blacklist pages to configure custom trusted and untrusted URLs and IPs. 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 “Sky Advanced Threat Prevention Whitelist and Blacklist Overview” on page 49 topic.
- Decide on the type of location you intend to define: URL or IP.
- Review current list entries to ensure the item you are adding does not already exist.

To create Sky ATP whitelists and blacklists:

1. Select **Configuration**.

The Whitelist landing page appears. You can remain on this page to create a whitelist or click **Blacklist** in the navigation pane.

2. When you create a new 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 table below.

3. Click **OK**.

Setting	Guideline
Domain	NOTE: Domains are not supported in this release. Enter a valid domain name such as juniper.net. It must begin with an alphanumeric character and can include colons, periods, dashes, and underscores; no spaces are allowed; 63-character maximum.
IP	Enter an IPV4 address in standard four octet format. CIDR notation and IP address ranges are also accepted. Any of the following formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6.
URL	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.

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

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.

**Related
Documentation**

- Sky Advanced Threat Prevention Whitelist and Blacklist Overview on page 49
- Enabling External Threat Feeds on page 81

CHAPTER 6

Email Scanning: Sky ATP

- Email Management Overview on page 53
- SMTP Quarantine Overview: Blocked Emails on page 55
- Email Management: Configure SMTP on page 56
- IMAP Block Overview on page 59
- Email Management: Configure IMAP on page 60
- Email Management: Configure Blacklists and Whitelists on page 62

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, 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.

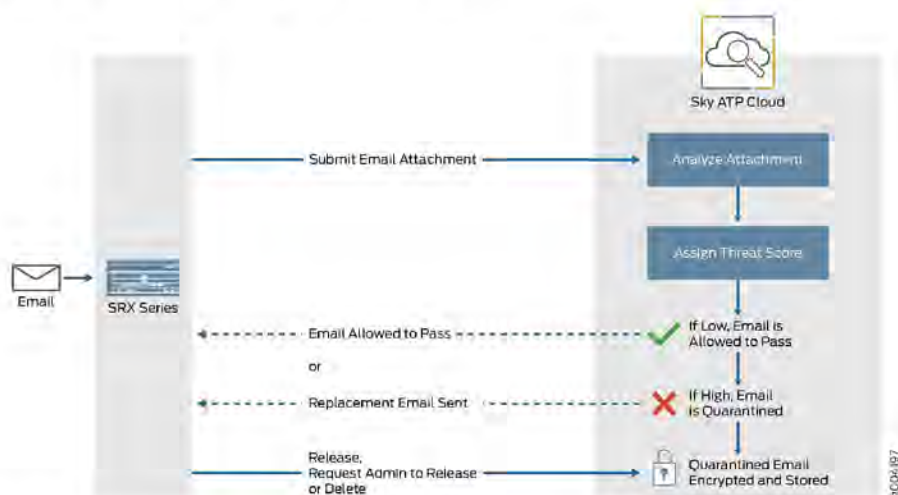
Configure Sky ATP to take one of the following actions when an email attachment is determined to be malicious:

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 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 19: 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 Sky ATP to have the recipient send a request to the administrator to release the email, the recipient previews the email in the 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 on page 56](#)
- [Email Management: Configure Blacklists and Whitelists on page 62](#)
- [SMTP Quarantine Overview: Blocked Emails on page 55](#)

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 10: 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.
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 Detail View:

Table 11: Blocked Email Detail View

Field	Description
Recipient	The email address of the recipient.
Sender	The email address of the sender.
Subject	Click the Read This link to go to the 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 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.

Table 11: Blocked Email Detail View (*continued*)

Field	Description
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

Note the following behavior regarding modes (permit and block) and blacklists and whitelists.

- In permit mode:
 - If an e-mail address is configured in the blacklist, the e-mail is downloaded to the client and is not sent to the cloud for scanning.
 - If an e-mail address is configured in the whitelist, the e-mail is downloaded to the client and is not sent to the cloud for scanning.
- In block mode:
 - If an e-mail address is configured in the blacklist, the e-mail is blocked and is not sent to the cloud for scanning.
 - If an e-mail address is configured in the whitelist, the e-mail is downloaded to the client and is not sent to the cloud for scanning.

- Related Documentation**
- [Email Management Overview on page 53](#)
 - [Email Management: Configure SMTP on page 56](#)
 - [HTTP File Download Overview on page 111](#)

Email Management: Configure SMTP

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

- Read the "Email Management Overview" on page 53 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 12: 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.
Release option	<ul style="list-style-type: none"> Recipients can release email—This option provides recipients with a link to the Sky ATP quarantine portal where they can preview the email. From the portal, recipients can select to Release the email or Delete it. Either action causes a message to be sent to the administrator. <p>NOTE: 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.</p> <ul style="list-style-type: none"> Recipients can request administrator to release email—This option also provides recipients with a link to the Sky ATP quarantine portal where they can preview the email. From the portal, recipients can select to Request to Release the email or Delete 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. <p>NOTE: 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.</p>
<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 Sky ATP quarantine portal link where recipients can preview quarantined emails and take action on them.
Buttons	<ul style="list-style-type: none"> Click Preview to view the custom message that will be sent to a recipient when an email is quarantined. Then click Save. Click Reset to clear all fields without saving. Click Save if you are satisfied with the configuration.

Table 13: 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"> • 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." • 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." • Subject Prefix—You can prepend headers with information for the recipient, such as "Possible Spam."
Buttons	<ul style="list-style-type: none"> • Click Reset to clear all fields without saving. • Click OK if you are satisfied with the configuration.

Table 14: 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 on page 53
- SMTP Quarantine Overview: Blocked Emails on page 55
- Configuring the SMTP Email Management Policy on the SRX Series Device on page 63

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 15: 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 16: Blocked Email Detail View

Field	Description
Recipient	The email address of the recipient.
Sender	The email address of the sender.
Subject	Click the Read This link to go to the 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 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 on page 60
- Email Management Overview on page 53

Email Management: Configure IMAP

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

- Read the "Email Management Overview" on page 53 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 17: Configure Block Malicious Messages

Setting	Guideline
Action to take	<ul style="list-style-type: none"> • Permit download of attachments—Allow email attachments, either from all IMAP servers or specific IMAP servers, through to their destination. <i>NOTE:</i> 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. • Block download of attachments—Block email attachments, either from all IMAP servers or specific IMAP servers, from reaching their destination. <i>NOTE:</i> 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. Recipients can send a request to an administrator to release the email. Enter the email address to which recipients should send a release request. <i>NOTE:</i> If a blocked email has multiple recipients, any individual recipient can request to release the email and all recipients will receive it. <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>

Table 17: Configure Block Malicious Messages (*continued*)

Setting	Guideline
IMAP Server	<ul style="list-style-type: none"> All IMAP Servers—The permitting or blocking of email attachments applies to all IMAP servers. 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. <p>When you add IMAP servers to the list, it is sent to the SRX Series device to filter emails sent to 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 Specific IMAP Server option above and click the + sign to add IMAP server hostnames to the list.</p> <p>NOTE: You must use the IMAP server hostname and not the IP address.</p>
<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 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 Sky ATP quarantine portal link where recipients can preview blocked emails and take action on them.
Buttons	<ul style="list-style-type: none"> Click Preview to view the custom message that will be sent to a recipient when an email is blocked. Then click Save. Click Reset to clear all fields without saving. Click Save if you are satisfied with the configuration.

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 on page 59
- Email Management Overview on page 53
- Configuring the IMAP Email Management Policy on the SRX Series Device on page 68

Email Management: Configure Blacklists and Whitelists

Access this page from the **Configure > Email Management** menu.

Use custom blacklists and whitelists to filter email according to administrator defined lists.

- Read the "Email Management Overview" on page 53 topic.
- Compile a list of known malicious email addresses or domains to add to your blacklist. 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, blocked and a replacement email is sent. If an email matches the whitelist, that email is allowed through without any scanning.
- 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.

The procedure for adding addresses to blacklists and whitelists is the same, although the results are very different. Be sure you are adding the entry to the correct list.

1. Select **Configure > Email Management > Whitelist or Blacklist**.
2. Click the **+** sign to add a new entry.
3. Enter the full address in the format **name@domain.com** or wildcard the name to permit or block all emails from a specific domain. For example, ***@domain.com**.
4. Click **OK**.

Related Documentation

- Enabling External Threat Feeds on page 81
- Email Management: Configure SMTP on page 56
- SMTP Quarantine Overview: Blocked Emails on page 55

CHAPTER 7

Email Scanning: SRX Series Device

- Configuring the SMTP Email Management Policy on the SRX Series Device on page 63
- Configuring the IMAP Email Management Policy on the SRX Series Device on page 68
- Configuring Reverse Proxy on the SRX Series Device on page 74

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 74.

```
# 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
  Session active: 52318
  Session blocked: 0
  Session permitted: 1354706
  Total HTTP HTTPS SMTP SMTPS
  52318 0 0 52318 0
  0 0 0 0 0
  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 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 smtppolicy1
```

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 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 74.

```
# 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 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 on page 59](#)
 - [Email Management: Configure IMAP on page 60](#)

Configuring Reverse Proxy on the SRX Series Device

Starting with Junos OS Release 15.1X49-D80, the SRX Series device acts as a proxy, so it can downgrade SSL negotiation to RSA. This was not possible in prior releases. Other changes are shown in Table 18 on page 74.

Table 18: Comparing Reverse Proxy Before and After Junos OS Release 15.1X49-D80

Feature	Prior to 15.1X49-D80	15.1X49-D80 and later
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 19 on page 75.

Table 19: Supported SSL Proxy Configurations

server-certificate configured	root-ca configured	Profile type
No	No	Commit check fails. You must configure either server-certificate or root-ca .
Yes	Yes	Commit check fails. Configuring both server-certificate and root-ca 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;
    }
  }
}
```

CHAPTER 8

File Inspection Profiles

- File Inspection Profiles Overview on page 77
- Creating File Inspection Profiles on page 79

File Inspection Profiles Overview

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

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.

Table 20: File Category Contents

Category	Description
Archive	Archive files
Configuration	Configuration files
Document	All document types except PDFs
Executable	Executable binaries
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 Sky ATP profile.



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

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 Sky ATP polling period.

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

**Related
Documentation**

- [Creating File Inspection Profiles on page 79](#)
- [Enrolling an SRX Series Device With Sky Advanced Threat Prevention on page 39](#)
- [Removing an SRX Series Device From Sky Advanced Threat Prevention on page 41](#)
- [Sky Advanced Threat Prevention License Types on page 11](#)

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 77 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 Sky Advanced Threat Prevention, you are limited to only the executable file category.

To create a device profile:

1. Select **Configure > File Inspection Profiles**.
2. Click the plus sign (+). Complete the configuration according to the guidelines provided in the table below.
3. Click **OK**.

Table 21: 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>Do not scan – This file type is not processed for scanning and is always allowed through.</p> <p>Hash lookup only – 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>Scan files up to max size – 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: 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 External Threat Feeds on page 81
- File Inspection Profiles Overview on page 77
- Sky Advanced Threat Prevention License Types on page 11

CHAPTER 9

External Threat Feeds

- Enabling External Threat Feeds on page 81

Enabling External Threat Feeds

Using this page, you can enable external feeds for integration with 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.
- Host analysis is optional for each feed. Host Analysis is used to determine if hosts that accessed items in threat feeds are infected. If hosts are found to be infected, they are added to infected hosts feed so they can be blocked. If you do not select Host Analysis for a feed, hosts with hits on that feed are not added to the list of infected hosts.

If you do not want to block hosts that have accessed items in an open source feed, but still want to view events for hits on the feed, you would not enable Host Analysis.



WARNING: Understand that these are open source feeds and determining the accuracy of the feed is left up to the Sky ATP administrator.

To enable the available feeds, do the following:

1. Navigate to **Configure > Threat Intelligence Feeds**.
2. For each feed, select the check box to enable the feed.
Click the **Details** link to view feed information, including the contents of the feed.
3. When a feed is enabled, the Host Analysis check box becomes available. Host Analysis is optional for each feed. (See the explanation of Host Analysis in the section above.)
4. 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 *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
```

5. 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 Sky ATP using the available CLI commands, refer to the *Sky Advanced Threat Prevention CLI Reference Guide*.

Related Documentation

- [Hosts Overview on page 91](#)
- [Host Details on page 93](#)
- [set services security-intelligence](#)

CHAPTER 10

Global Configurations

- [Global Alert Configuration Overview on page 85](#)
- [Creating and Editing the Global Alert Configuration on page 85](#)
- [Configuring Threat Intelligence Sharing on page 86](#)
- [Configuring Trusted Proxy Servers on page 88](#)

Global Alert Configuration Overview

You can configure Sky ATP to send e-mails 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.

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.

From this page, you can also select which event types to log: Malware events and Host Status events.

Related Documentation

- [Creating and Editing the Global Alert Configuration on page 85](#)
- [Modifying My Profile on page 139](#)
- [Creating and Editing User Profiles on page 140](#)

Creating and Editing the Global Alert Configuration

Use this page to set a global alert threshold level, which when reached, triggers an alert to all listed e-mail addresses.

- Review the “Global Alert Configuration Overview” on page 85 topic.
- Decide which users will receive notifications. It might not be necessary for all users to receive alerts.

To create or update the global settings:

1. Select **Configure > Global Configuration**.
2. (Premium licenses only) Set the default threat level threshold.
3. Select which event types to log. To log all Malware events, select **Malware** check box. To log all Host Status events, select the **Host Status** check box.
4. 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.
5. Click **OK**.

Table 22: Global Configuration Fields

Setting	Guideline
E-mail	Enter an e-mail address.
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.

- Related Documentation**
- [Global Alert Configuration Overview on page 85](#)
 - [Modifying My Profile on page 139](#)
 - [Creating and Editing User Profiles on page 140](#)

Configuring Threat Intelligence Sharing

Using the TAXII service, Sky ATP can contribute to STIX reports by sharing the threat intelligence it gathers from file scanning. Sky ATP also uses threat information from STIX reports as well as other sources for threat prevention. See "HTTP File Download Details" on page 112 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 141.

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 slidebar 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 141.

Table 23: 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: taxii-discovery</p> <p>NOTE: Refer to the TAXII documentation for information on additional commands. http://taxiiproject.github.io/documentation/</p> <p>Sky ATP Discovery URLs are:</p> <p>US Region: https://taxii.sky.junipersecurity.net/services/discovery</p> <p>EU Region: https://taxii-eu.sky.junipersecurity.net/services/discovery</p>
At this time, there are two services supported by Sky ATP on the TAXII server.	
Collection Management	<p>Used by the TAXII client to request information about available data collections.</p> <p>Sky ATP Collection Management URLs are:</p> <p>US Region: https://taxii.sky.junipersecurity.net/services/collection-management</p> <p>EU Region: https://taxii-eu.sky.junipersecurity.net/services/collection-management</p>
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>Sky ATP Polling URLs are:</p> <p>US Region: https://taxii.sky.junipersecurity.net/services/poll</p> <p>EU Region: https://taxii-eu.sky.junipersecurity.net/services/poll</p>

- Related Documentation**
- HTTP File Download Details on page 112
 - Creating Application Tokens on page 141

Configuring Trusted Proxy Servers

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

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 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, 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 on page 91](#)
- [Compromised Hosts: More Information on page 95](#)

PART 4

Monitor and Take Action

- Hosts on page 91
- Identifying Infected Hosts on page 95
- Command and Control Servers on page 103
- Identify Hosts Communicating with Command and Control Servers on page 107
- File Scanning on page 111
- Email Scanning on page 119

CHAPTER 11

Hosts

- Hosts Overview on page 91
- Host Details on page 93

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.

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.

For the Hosts listed on this page, you can perform the following actions on one or multiple hosts at once:

Table 24: 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.
Select Policy Override	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.
Select 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.

Table 24: Operations for Multiple Infected Hosts (*continued*)

Action	Definition
<p>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.</p>	

The following information is available in the Host table.

Table 25: Compromised Host Information

Field	Description
Host Identifier	<p>The Sky ATP-assigned name for the host. This name is created by 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: username@server. 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>user01@aa:bb:cc:dd:ee:ff, user02@1.1.1.1 or 1.1.1.1</p> <p>NOTE: You can edit this name. If you edit the Sky ATP-assigned name, Sky ATP will recognize the new name and not override it.</p>
Host IP	The IP address of the compromised host.
Threat Level	<p>A number between 0 -10 indicating the severity of the detected threat, with 10 being the highest.</p> <p>NOTE: 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"> • Included: This is the default policy. The host is included in the infected host feed if its threat level meets the set infected host threshold. • Excluded: The host is whitelisted and will be excluded from the infected host feed even if its threat level meets the threshold. • Included Manually: The host is blacklisted and will be included in infected host feed even if its threat level does not meet the threshold.
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>NOTE: Click the three vertical dots at the top of the column to filter the information on the page by C&C hits.</p>
Malware	<p>The number of times a malware threat was downloaded by this host.</p> <p>NOTE: Click the three vertical dots at the top of the column to filter the information on the page by malware detections.</p>

Table 25: Compromised Host Information (*continued*)

Field	Description
State of Investigation	Displays either Open, In progress, Resolved-False positive, Resolved-Fixed, Resolved-Ignored

- Related Documentation**
- Host Details on page 93
 - HTTP File Download Overview on page 111
 - HTTP File Download Details on page 112
 - Manual Scanning Overview on page 115

Host Details

Access this page by clicking the Host Identifier from the **Monitor > Hosts** page.

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 26: 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.

- **Assigned Name**—Displays the 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 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 on page 91](#)
- [HTTP File Download Overview on page 111](#)
- [HTTP File Download Details on page 112](#)
- [Manual Scanning Overview on page 115](#)

CHAPTER 12

Identifying Infected Hosts

- [Compromised Hosts: More Information on page 95](#)
- [Configuring the SRX Series Devices to Block Infected Hosts on page 101](#)

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:

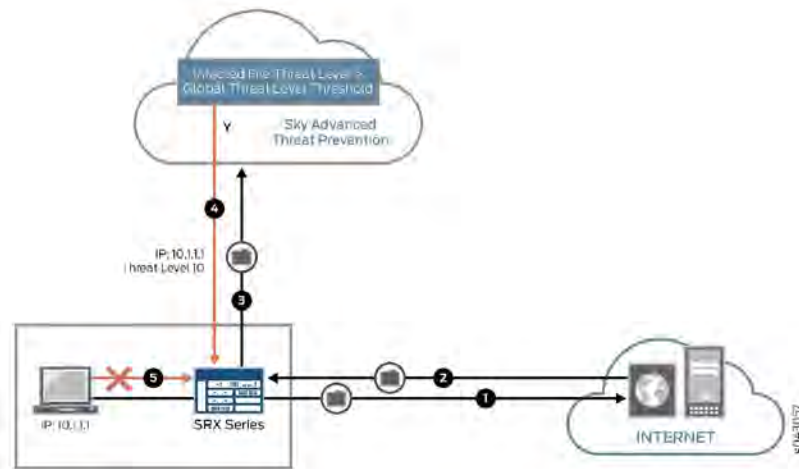
- Send junk or spam e-mail to attack other systems or distribute illegal software.
- Collect personal information, such as passwords and account numbers.
- Disable your computer's security settings to allow easy access.

In Sky ATP, infected hosts are listed as data feeds (also called information sources). The feed lists the 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, 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. 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 Sky Advanced Threat Prevention Script" on page 23.

Figure 20 on page 96 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 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 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	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 monitor hosts as shown in Figure 21 on page 97.

Figure 21: Viewing Infected Hosts

Host	Threat Level	Policy Name	Download Date	Threat Last Seen	OS Type	Session Pkts	Host IP/hostname
192.0.2.10	10	Block	Jan 15, 2016 4:47 PM	Jan 15, 2016 4:27 PM	Windows	0	192.0.2.10
192.0.2.10	10	Block	Dec 21, 2015 8:59 AM	Jan 21, 2016 1:59 PM	Windows	113	192.0.2.10
192.0.2.10	10	Block	Dec 22, 2015 9:02 PM	Jan 19, 2016 4:22 PM	Windows	70	192.0.2.10
192.0.2.10	10	Block	Dec 30, 2015 9:35 AM	Jan 20, 2016 12:30 PM	Windows	74	192.0.2.10
192.0.2.10	10	Block	Dec 31, 2015 1:32 PM	Jan 20, 2016 3:50 PM	Windows	0	192.0.2.10
192.0.2.10	10	Block	Jan 4, 2016 8:57 AM	Jan 20, 2016 2:14 PM	Windows	120	192.0.2.10
192.0.2.10	10	Block	Dec 30, 2015 8:30 PM	Jan 22, 2016 12:42 PM	Windows	0	192.0.2.10

You can also use the `show services security-intelligence statistics` CLI command 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** tab 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 *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 in_progress .
host_policy	Name of 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: Added, Cleared, Present, Absent .
reason	Reason for the log entry. It can be one of the following: Malware, CC, Manual .
details	Brief description of the entry reason, for example: malware analysis detected host downloaded a malicious_file with score 9, sha256 abc123

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 101.

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

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 and a threat level, for example xxx.xxx.xxx.133 with threat level 5. 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.

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
```

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.

CHAPTER 13

Command and Control Servers

- Command and Control Servers Overview on page 103
- Command and Control Server Details on page 104

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 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. 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 intelligence feed information that identifies the C&C server IP address and URL.

- **Export Data**—Click the **Export** button to download C&C data to a CSV file. You are prompted to narrow the data download to a selected time-frame.
- **Report False Positives**—Click the **FP/FN** 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.

The following information is available on this page.

Table 27: 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 on page 104](#)
 - [Host Details on page 93](#)
 - [Hosts Overview on page 91](#)

Command and Control Server Details

Access this page by clicking the **External Server IP** 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

You can filter this information by clicking on the time-frame links: 1 day, 1 week, 1 month, Custom (select your own time-frame). You can also expand the time-frame to separate events using the slider.

Hosts That have Contacted This C&C Server

This is a list of hosts that have contacted the server. The information provided in this section is as follows:

Table 28: 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.
Action	The action taken on the communication (permitted or blocked).
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.

Associated Domains

Table 29: Command & 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

This is a list of command and control indicators that were detected.

Table 30: Command & 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 on page 103](#)
 - [Host Details on page 93](#)
 - [Hosts Overview on page 91](#)

CHAPTER 14

Identify Hosts Communicating with Command and Control Servers

- [Command and Control Servers: More Information](#) on page 107
- [Configuring the SRX Series Device to Block Outbound Requests to a C&C Host](#) on page 109

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 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, 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**).

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://xxx.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 on page 109](#)

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 on page 107](#)

CHAPTER 15

File Scanning

- HTTP File Download Overview on page 111
- HTTP File Download Details on page 112
- Manual Scanning Overview on page 115
- File Scanning Limits on page 116

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.



NOTE: When managing Sky ATP with Security Director, you must select a Sky ATP realm from the available pulldown.

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 31: 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.
Threat Level	The threat score. NOTE: Click the three vertical dots at the top of the column to filter the information on the page by threat level.

Table 31: HTTP Scanning Data Fields (*continued*)

Field	Definition
Filename	The name of the file, including the extension. NOTE: 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. NOTE: 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." NOTE: Enter text in the space at the top of the column to filter the data.
Category	The type of file. Examples: PDF, executable, document. NOTE: Enter text in the space at the top of the column to filter the data.

Related Documentation

- [Email Attachments Scanning Overview on page 119](#)
- [File Scanning Limits on page 116](#)
- [HTTP File Download Details on page 112](#)
- [Manual Scanning Overview on page 115](#)
- [Hosts Overview on page 91](#)
- [Host Details on page 93](#)

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 32: Links on the HTTP File Download Details Page

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.

Table 32: Links on the HTTP File Download Details Page (*continued*)

Link	Purpose
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. 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>NOTE: 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 86.</p>
Download Zipped Files	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 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 33: 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.

Table 33: General Summary Fields (continued)

Field	Definition
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe., wordmul.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, Sky ATP determines the name of the malware.
Malware Type	If possible, Sky ATP determines the type of threat. Example: Trojan, Application, Adware.
Malware Strain	If possible, 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 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 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 22: Sample STIX Report

```

<?xml version="1.0" ?>
<stix:STIX_Package version="1.2" id="examplePackage-a8bc14e2-b392-4ea0-b40f-0a03aaaa0cb3" xmlns:WinProcessObj="http://cybox.mitre.org/objects/WinProcessObject-2"
xmlns:os="http://www.w3.org/2001/XMLSchema" xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects/WinRegistryKeyObject-2" xmlns:ids="http://stix.mitre.org/stix-1"
xmlns:stixVocab="http://stix.mitre.org/default_vocabularies-1" xmlns:WinThreadObj="http://cybox.mitre.org/objects/WinThreadObject-2" xmlns:simple="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:idsa="http://www.w3.org/1999/xmldsig" xmlns:inst="http://www.w3.org/2001/XMLSchema-instance"
xmlns:fileObj="http://cybox.mitre.org/objects/FileObject-2" xmlns:cyboxVocab="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:ids="http://www.w3.org/2000/06/xmldsig#">
  <stix:STIX_Header>
    <stix:Description> IOCs for sample id: a9c097d0f6392897f87764d43ac9ad4b60078f7062325b7798909e484f3f1af </stix:Description>
  </stix:STIX_Header>
  <stix:Indicators>
    <stix:Indicator id="exampleIndicator-92000f82-82b0-45bf-9ac7-bf4566c1c93d" xsi:type="indicatorIndicatorType" timestamp="2017-10-09T20:31:25.918941+00:00">
      <indicator:Title> File Indicator(s) for sample a9c097d0f6392897f87764d43ac9ad4b60078f7062325b7798909e484f3f1af </indicator:Title>
      <indicator:Description> An indicator containing file observable(s) </indicator:Description>
      <indicator:Observable id="exampleObservable-907ee5c7-0c06-414c-a096-f3199d3aa0fb">
        <cybox:Object id="exampleFile-a8bc14e2-b392-4ea0-b40f-0a03aaaa0cb3">
          <cybox:Properties xsi:type="FileObj:FileType">
            <FileObj:Hashes>
              <cybox:Common:Hash>
                <cybox:Common:Type xsi:type="cyboxVocab:hashNameVocab-1.0"> MD5 </cybox:Common:Type>
                <cybox:Common:Simple_Hash_Value> b941993d05ad814dc9b7d35fec3f0ae61 </cybox:Common:Simple_Hash_Value>
              </cybox:Common:Hash>
              <cybox:Common:Hash>
                <cybox:Common:Type xsi:type="cyboxVocab:hashNameVocab-1.0"> SHA1 </cybox:Common:Type>
                <cybox:Common:Simple_Hash_Value> e70f1bb911ee60ef0e7aa2c423eaa5a04d17e709 </cybox:Common:Simple_Hash_Value>
              </cybox:Common:Hash>
              <cybox:Common:Hash>
                <cybox:Common:Type xsi:type="cyboxVocab:hashNameVocab-1.0"> SHA256 </cybox:Common:Type>
                <cybox:Common:Simple_Hash_Value> a9c097d0f6392897f87764d43ac9ad4b60078f7062325b7798909e484f3f1af </cybox:Common:Simple_Hash_Value>
              </cybox:Common:Hash>
              <cybox:Common:Hash>
                <cybox:Common:Type xsi:type="cyboxVocab:hashNameVocab-1.0"> SHA512 </cybox:Common:Type>
                <cybox:Common:Simple_Hash_Value> 14fc2d6a088a3bb617726a9cc4c428da9c874ef21c98538651b6d537b5e8d60a2c40b2d20740146c9a8f177
              </cybox:Common:Hash>
            </FileObj:Hashes>
          </cybox:Properties>
        </cybox:Object>
      </indicator:Observable>
    </stix:Indicator>
  </stix:Indicators>
</stix:STIX_Package>

```

Related Documentation

- File Scanning Limits on page 116
- HTTP File Download Overview on page 111
- Manual Scanning Overview on page 115
- Hosts Overview on page 91

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.

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 Sky ATP premium-licensed SRX Series devices and one other SRX Series device, 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 Sky ATP in order to use the manual file scanning feature.

Table 34: 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 on page 91
 - HTTP File Download Overview on page 111
 - HTTP File Download Details on page 112
 - Email Attachments Scanning Overview on page 119
 - Email Attachments Scanning Details on page 120

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

Perimeter Device	Free License (files per day)	Premium License (files per day)
SRX1500	2,500	10,000
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 on page 111](#)
 - [Email Attachments Scanning Overview on page 119](#)
 - [Manual Scanning Overview on page 115](#)

CHAPTER 16

Email Scanning

- [Email Attachments Scanning Overview](#) on page 119
- [Email Attachments Scanning Details](#) on page 120

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.



NOTE: When managing Sky ATP with Security Director, you must select a Sky ATP realm from the available pulldown.

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 35: 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.
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.

Table 35: Email Attachments Scanning Data Fields (continued)

Field	Definition
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 on page 120](#)
- [File Scanning Limits on page 116](#)
- [HTTP File Download Overview on page 111](#)
- [HTTP File Download Details on page 112](#)
- [Hosts Overview on page 91](#)
- [Host Details on page 93](#)

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 Zipped Files—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 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 36: 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.msl.
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, Sky ATP determines the name of the malware.
Malware Type	If possible, Sky ATP determines the type of threat. Example: Trojan, Application, Adware.
Malware Strain	If possible, 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 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 on page 111](#)
- [HTTP File Download Details on page 112](#)
- [Email Attachments Scanning Overview on page 119](#)
- [Manual Scanning Overview on page 115](#)
- [SMTP Quarantine Overview: Blocked Emails on page 55](#)

PART 5

Policies on the SRX Series Device

- Configure Sky ATP Policies on the SRX Series Device on page 125
- Configure IP-Based Geolocations on the SRX Series Device on page 133

CHAPTER 17

Configure Sky ATP Policies on the SRX Series Device

- Sky Advanced Threat Prevention Policy Overview on page 125
- Enabling Sky ATP for Encrypted HTTPS Connections on page 128
- Example: Configuring a Sky Advanced Threat Prevention Policy Using the CLI on page 129

Sky Advanced Threat Prevention Policy Overview

The connection to the 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 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.

Sky ATP policies are an extension to the Junos OS security policies. Table 37 on page 126 shows the additions.



NOTE: Starting in Junos OS Release 15.1X49-D80, the match-then condition has been deprecated from the Sky ATP policy configuration. For more information, see 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 37: 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 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 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 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"> • action—Permit or block the file regardless of its threat level. • notification—Add or do not add this event to the log file. <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>NOTE: The above actions assume a valid session is present. If no valid session is present, 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>
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 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 Sky Advanced Threat Prevention Policy Using the CLI" on page 129.

Enabling 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 Sky Advanced Threat Prevention Policy Using the CLI" on page 129.

Related Documentation

- [Example: Configuring a Sky Advanced Threat Prevention Policy Using the CLI on page 129](#)

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

This example shows how to create a Sky ATP policy using the CLI. It assumes you understand configuring security zones and security policies. See [Example: Creating Security Zones](#).

- Requirements on page 129.
- Overview on page 129
- Configuration on page 130
- Verification on page 132

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 Sky ATP policy configuration. For more information, see [Sky Advanced Threat Prevention Release Notes for Junos 15.1X49-D80](#). This example includes those updates.

Overview

This example creates a 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 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 [Sky ATP Release Notes \(for Junos 15.1X49-D80\)](#).

1. Create the 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 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 Sky ATP for Encrypted HTTPS Connections” on page 128 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
```

CHAPTER 18

Configure IP-Based Geolocations on the SRX Series Device

- Geolocation IPs and Sky Advanced Threat Prevention on page 133
- Configuring Sky Advanced Threat Prevention With Geolocation IP on page 134

Geolocation IPs and 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. 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 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 Sky Advanced Threat Prevention Script" on page 23.

Currently, configuring GeoIP and security policies is done completely on the SRX Series device using CLI commands.

Related Documentation

- Configuring Sky Advanced Threat Prevention With Geolocation IP on page 134

Configuring Sky Advanced Threat Prevention With Geolocation IP

To configure 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-geoup-policy {
    match {
      source-address my-geoup;
      destination-address any;
      application any;
    }
    then {
      deny;
    }
  }
}
...
```

Related Documentation • [Geolocation IPs and Sky Advanced Threat Prevention on page 133](#)

PART 6

Administration

- Sky ATP Administration on page 139

CHAPTER 19

Sky ATP Administration

- Modifying My Profile on page 139
- Creating and Editing User Profiles on page 140
- Application Tokens Overview on page 141
- Creating Application Tokens on page 141

Modifying My Profile

An administrator profile is created for you when you register for a 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 38: 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.

Table 38: My Profile Fields (*continued*)

Setting	Guideline
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 Sky ATP is your e-mail address.

- Related Documentation**
- [Creating and Editing User Profiles on page 140](#)
 - [Reset Password on page 37](#)

Creating and Editing User Profiles

Use this page to create additional user accounts or modify existing accounts for Sky ATP. Multiple users can log into Sky ATP at the same time.

- Review the "Modifying My Profile" on page 139 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 39: User 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 Sky ATP is your e-mail address.
Confirm Password	Re-enter the password.

- Related Documentation**
- [Modifying My Profile on page 139](#)

Application Tokens Overview

Use the App Token page to view application tokens that allow Security Director or Open API users to securely access 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.

- Related Documentation**
- [Creating Application Tokens on page 141](#)

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 141 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 40 on page 142](#) 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 40: 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 an 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 on page 141](#)
- [Command and Control Servers Overview on page 103](#)

PART 7

Troubleshoot

- Troubleshooting Topics on page 145

CHAPTER 20

Troubleshooting Topics

- [Sky Advanced Threat Prevention Troubleshooting Overview on page 145](#)
- [Troubleshooting Sky Advanced Threat Prevention: Checking DNS and Routing Configurations on page 146](#)
- [Troubleshooting Sky Advanced Threat Prevention: Checking Certificates on page 148](#)
- [Troubleshooting Sky Advanced Threat Prevention: Checking the Routing Engine Status on page 149](#)
- [request services advanced-anti-malware data-connection](#)
- [request services advanced-anti-malware diagnostic](#)
- [Troubleshooting Sky Advanced Threat Prevention: Checking the application-identification License on page 156](#)
- [Viewing Sky Advanced Threat Prevention System Log Messages on page 156](#)
- [Configuring traceoptions on page 157](#)
- [Viewing the traceoptions Log File on page 159](#)
- [Turning Off traceoptions on page 159](#)
- [Sky Advanced Threat Prevention Dashboard Reports Not Displaying on page 160](#)
- [Sky Advanced Threat Prevention RMA Process on page 160](#)

Sky Advanced Threat Prevention Troubleshooting Overview

This topic provides a general guide to troubleshooting some typical problems you may encounter on Sky ATP.

Table 41 on page 146 provides a summary of the symptom or problem and recommended actions with links to the troubleshooting documentation.

Table 41: Troubleshooting Sky ATP

Symptom or Problem	Recommended Action
SRX device can't communicate with cloud	<p>See "Troubleshooting Sky Advanced Threat Prevention: Checking DNS and Routing Configurations" on page 146</p> <p>See "Troubleshooting Sky Advanced Threat Prevention: Checking Certificates" on page 148</p> <p>See "Troubleshooting Sky Advanced Threat Prevention: Checking the Routing Engine Status" on page 149</p> <p>See <code>request services advanced-anti-malware data-connection</code></p> <p>See <code>request services advanced-anti-malware diagnostic</code></p>
Files not being sent to cloud	<p>See "Troubleshooting Sky Advanced Threat Prevention: Checking DNS and Routing Configurations" on page 146</p> <p>See "Troubleshooting Sky Advanced Threat Prevention: Checking Certificates" on page 148</p> <p>See "Troubleshooting Sky Advanced Threat Prevention: Checking the Routing Engine Status" on page 149</p> <p>See "Troubleshooting Sky Advanced Threat Prevention: Checking the application-identification License" on page 156</p>
Viewing system log messages	See "Viewing Sky Advanced Threat Prevention System Log Messages" on page 156
Setting traceoptions	<p>See "Configuring traceoptions" on page 157</p> <p>See "Viewing the traceoptions Log File" on page 159</p> <p>See "Turning Off traceoptions" on page 159</p>
Dashboard reports not displaying any data	See "Sky Advanced Threat Prevention Dashboard Reports Not Displaying" on page 160

Troubleshooting 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 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: xxxxxxxxxx
Issuer:
  Organization: Juniper Networks Inc, Organizational unit: SecIntel, Country:
US,
  Common name: SecIntel (junipersecurity.net) subCA for SRX devices
Subject:
  Organization: xxxxxxxxxx, Organizational unit: SRX, Country: US,
  Common name: xxxxxxxxxx
Subject string:
  C=US, O=xxxxxxx, OU=SRX, CN=xxxxxxx, 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
  xxxxxxxxxxxxxxxxxxxx  10-26-2015 17:43 UTC
  xxxxxxxxxxxxxxxxxxxx  11- 3-2015 19:07 UTC
  ...
```

Troubleshooting 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 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 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 42 on page 151.

Required Privilege Level View

Related Documentation

- [request services advanced-anti-malware diagnostic on page 153](#)

List of Sample Output

- [request services advanced-anti-malware data-connection test start on page 152](#)
- [request services advanced-anti-malware data-connection test status on page 152](#)
- [request services advanced-anti-malware data-connection test status on page 152](#)

Output Fields This CLI command returns a single line that indicates the data connection results. Table 42 on page 151 lists the possible results.

Table 42: Data Connection Test Output

Message	Description
Test not started.	You cannot view the status without first running the data connection test. Run the request services advanced-anti-malware data-connection test start 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.

Table 42: Data Connection Test Output (*continued*)

Message	Description
Test failed.	<p>The data connection test failed and indicates where it failed. Possible failures are:</p> <ul style="list-style-type: none"> • Connect error—The websocket connection cannot be established. • Ping pong error—Successfully connected to the cloud server, but the payload delivery is not reliable.

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 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 43 on page 154.

Options *url*—URL to the 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.s1ax
```

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 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 43 on page 154 lists the error conditions detected by this CLI command.

Table 43: 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.
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.

Table 43: aamw-diagnostics Script Error Messages (*continued*)

Error Message	Description
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 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 on page 151](#)

List of Sample Output [request services advanced-anti-malware diagnostic on page 155](#)
[request services advanced-anti-malware diagnostic detail on page 155](#)
[request services advanced-anti-malware diagnostic pre-detection on page 156](#)

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 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 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. 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.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 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.

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 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.

Sky Advanced Threat Prevention Dashboard Reports Not Displaying

Sky ATP dashboard reports require the 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: 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 Sky Advanced Threat cloud server. For more information, see *Obtaining the Sky Advanced Threat Prevention License*.

All reports are specific to your realm; no report currently covers trends derived from the 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 "Sky Advanced Threat Prevention Configuration Overview" on page 31) and are still not seeing data in the dashboard reports, contact Juniper Networks Technical Support.

Sky Advanced Threat Prevention RMA Process

Sometimes, 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 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 Sky ATP cloud. This means that you must enroll your replacement unit as a new device. See "Enrolling

an SRX Series Device With Sky Advanced Threat Prevention” on page 39. 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.

PART 8

More Documentation

- Sky ATP Tech Library Page Links on page 165

CHAPTER 21

Sky ATP Tech Library Page Links

- [Links to Documentation on Juniper.net](#) on page 165

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.

