JUNIPER NETWORKS

Sky Advanced Threat Prevention Guide

Modified: 2016-08-02

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Sky Advanced Threat Prevention Guide

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.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation ix
Documentation and Release Notes ix
Documentation Conventions ix
Documentation Feedback xi
Requesting Technical Support xii
Self-Help Online Tools and Resources xii
Opening a Case with JTAC xii

Chapter 1 **Overview 15**

Sky Advanced Threat Prevention Overview 16
Sky Advanced Threat Prevention Features 17
Sky Advanced Threat Prevention Components 18
Remediation and Malware Detection Overview 19
How Malware Is Analyzed and Detected 19
Cache Lookup 20
Antivirus Scan 20
Static Analysis 20
Dynamic Analysis 20
Machine Learning Algorithm 21
Sky ATP Licensed Features and File Scanning Limits 21
File Scanning Limits 22

Chapter 2 **Dashboard 25**

Dashboard Overview 25

Chapter 3 **Monitor 27**

Hosts Overview 27
Host Details 28
Command and Control Servers Overview 29
File Scanning Overview 30
File Scanning Details 31
File Summary 31
Hosts That have Downloaded the File 31
Malware Behavior Summary 32
File Scanning Limits 32
Manual Scanning Overview 33

Chapter 4 **Devices 35**

Enrolled Devices 35
Enrolling and Disenrolling Devices 36
Device Lookup Overview 38
Device Information 38

Chapter 5 Configure 41
Custom Whitelist and Blacklist Overview 41
Creating Whitelists and Blacklists 42
Device Profiles Overview 43
Creating Device Profiles 44
Chapter 6 Administration 47
Modifying My Profile 47
User Profiles Overview 48
Creating and Editing User Profiles 48
Global Configuration Overview 49
Creating and Editing Global Configurations 49
Chapter 7 More information 51
Links to Documentation on Juniper.net 51
Chapter 8 Index 53
Index 55

List of Figures

Chapter 1 **Overview** 15

Figure 1: Sky Advanced Threat Prevention Overview 16

Figure 2: Example Sky Advanced Threat Prevention Pipeline Approach for Analyzing Malware 19

Chapter 3 **Monitor** 27

Figure 3: Screen Capture: Malicious Behavior Summary 32

List of Tables

About the Documentation ix

Table 1: Notice Icons x
Table 2: Text and Syntax Conventions x

Chapter 1 Overview 15

Table 3: Tabs and What Their Workspaces Access 17
Table 4: Sky Advanced Threat Prevention Components 18
Table 5: Comparing the Sky Advanced Threat Prevention Free Model and Premium Model 22
Table 6: File Scanning Limits 23

Chapter 2 Dashboard 25

Table 7: Sky ATP Dashboard Widgets 25

Chapter 3 Monitor 27

Table 8: Threat Level Definitions 28
Table 9: Command & Control Server Data Fields 29
Table 10: File Scanning Data Fields 30
Table 11: File Summary Fields 31
Table 12: File Scanning Limits 32
Table 13: File Scanning Data Fields 33

Chapter 4 Devices 35

Table 14: Button Actions 35
Table 15: Device Information Fields 39

Chapter 5 Configure 41

Table 16: Whitelist and Blacklist: Domain, IP, and URL Required Information and Syntax 42
Table 17: File Category Contents 43
Table 18: Device Profile Settings 45

Chapter 6 Administration 47

Table 19: My Profile Fields 48
Table 20: User Fields 49
Table 21: Global Configuration Fields 50

About the Documentation

- Documentation and Release Notes on page ix
- Documentation Conventions on page ix
- Documentation Feedback on page xi
- Requesting Technical Support on page xii

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 x 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 x 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**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	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** *domain-name*

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.	• 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 *metric*>;**
| (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** **(*string1* | *string2* | *string3*)**
# (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 [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  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.	• 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: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

CHAPTER 1

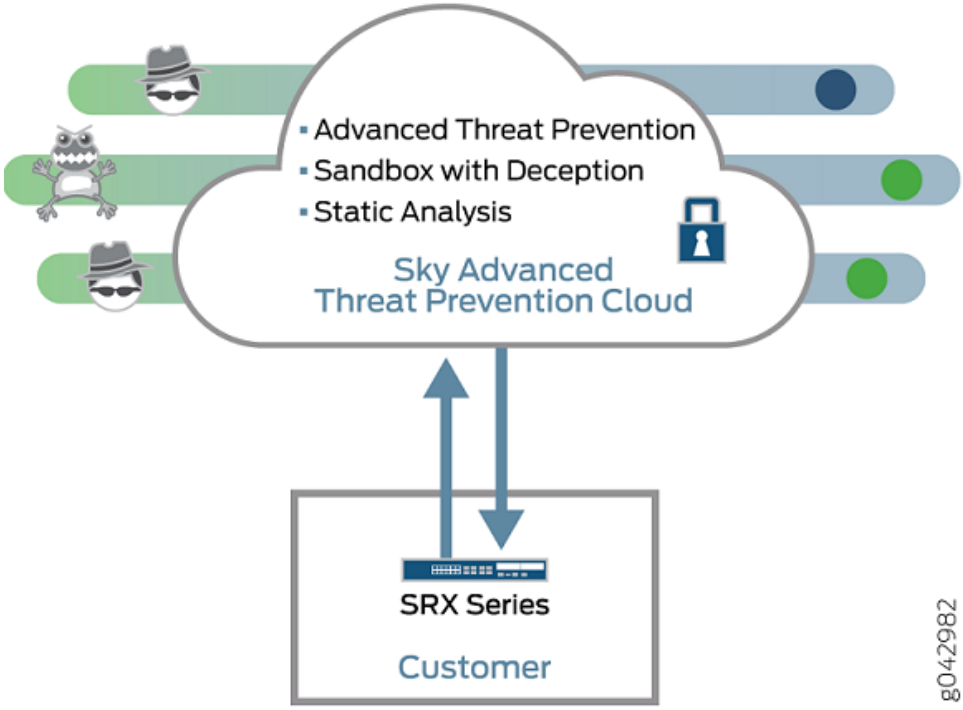
Overview

- Sky Advanced Threat Prevention Overview on page 16
- Remediation and Malware Detection Overview on page 19
- Sky ATP Licensed Features and File Scanning Limits on page 21

Sky Advanced Threat Prevention Overview

Juniper Networks Sky Advanced Threat Prevention 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.

Figure 1: Sky Advanced Threat Prevention Overview



Sky Advanced Threat Prevention 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.

The Web UI is hosted by Juniper Networks in the cloud. The tabs across the top of the web UI provide workspaces in which an administrator can perform specific tasks. Table 1 shows the names of the tabs along with brief descriptions of what is accessible in that workspace.

Table 3: Tabs and What Their Workspaces Access

Tab Name	Accesses
Dashboard	Provides graphical widgets that can be added, removed, and rearranged on a per-user basis. These widgets offer each user a customized view of malware detection categorized in a variety of ways.
Monitor	Provides information on the following: • Malware detection status for registered hosts • C&C servers that have attempted to contact and compromise hosts on your network. • Files downloaded by hosts that are suspicious
Devices	Lists all devices that have been registered with Sky ATP. From here you can: • Enroll new devices • Disenroll devices • Search for devices in the list by their serial number
Configure	Configure the following: • Whitelists—Add your own trusted IP addresses, URLs, and domains to the global items in the whitelist. • Blacklists—Add your own untrusted IP addresses, URLs, and domains to the global items in the blacklist. • Devices profiles—Group types of files to be scanned together under a common name.
Administration	Edit your user profile and create new user profiles. You can also: • Change user passwords • Set a global alert threshold level, which when reached, triggers an alert to all listed e-mail addresses

Sky Advanced Threat Prevention Features

Sky Advanced Threat Prevention 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 Advanced Threat Prevention 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 compromised systems, prevent data exfiltration, and disrupt lateral movement. High availability provides 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

Sky Advanced Threat Prevention Components

The following table describes how the components of the Sky Advanced Threat Prevention solution work together.

Table 4: Sky Advanced Threat Prevention Components

Component	Description
Security intelligence cloud feeds	A feed distribution point that delivers feeds to the SRX Series device. These include: • C&C • Compromised hosts • GeoIP • Whitelists and blacklists C&C feeds are essentially a list of servers that are known Command and Control servers for botnets. The list also includes servers that are known sources for malware downloads. Compromised hosts, or infected hosts, indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms. 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. A whitelist is a list of known IP addresses that you trust, and a blacklist is a list that you do not trust. NOTE: C&C and GeoIP filtering feeds are only available with a Premium license. For information on licensed features, see Sky ATP Licensing.
SRX Series device	Submits extracted file content for analysis and detected C&C hits inside the customer network. Performs inline blocking based on verdicts from the analysis cluster.
Malware inspection pipeline	Performs malware analysis and threat detection.
Internal compromise detection	Inspects files,metadata, and other information.
Service portal (Web UI)	Graphics interface displaying information about detected threats inside the customer network. Configuration management tool where customers can fine-tune which file categories can be submitted into the cloud for processing.

Related Documentation

- Dashboard Overview on page 25
- *Sky Advanced Threat Prevention Licenses*
- Hosts Overview on page 27

- File Scanning Overview on page 30
- Command and Control Servers Overview on page 29

Remediation and Malware Detection Overview

The SRX Series devices use intelligence provided by Sky Advanced Threat Prevention 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.

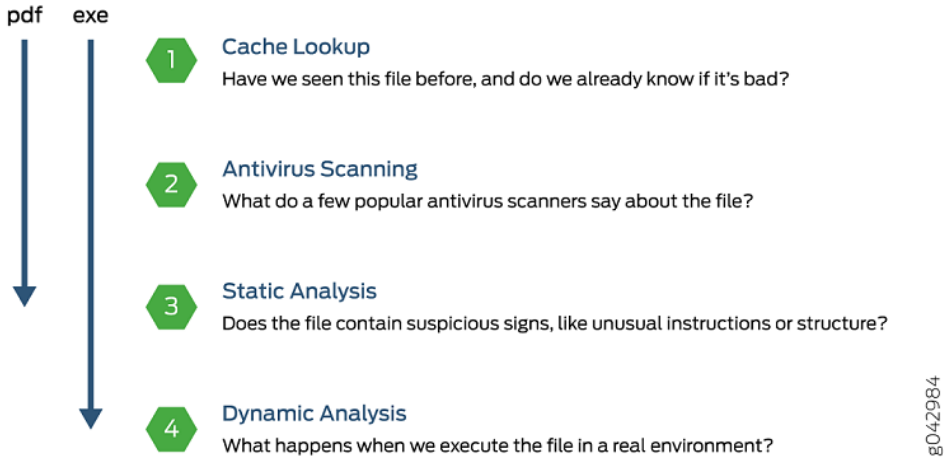
For inbound traffic, security policies on the SRX Series device look for specific types of files, like .exe files, to inspect. When one is encountered, the security policy sends the file to the Sky Advanced Threat Prevention cloud for inspection. The SRX Series device holds the last few kilobytes of the file from the destination client until Sky Advanced Threat Prevention provides a verdict. If Sky Advanced Threat Prevention returns a bad verdict, the SRX Series device drops the connection and the file is blocked.

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

How Malware Is Analyzed and Detected

Sky Advanced Threat Prevention 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.

Figure 2: Example Sky Advanced Threat Prevention Pipeline Approach for Analyzing Malware



Each analysis technique creates a verdict number, which is combined to create a final verdict number from 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 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 Advanced Threat Prevention 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 Advanced Threat Prevention, 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 Advanced Threat Prevention 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 Advanced Threat Prevention 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 that static analysis inspects:

- Metadata information—Name of the file, the vendor or creator of this file, and the original data on which the file was compiled.
- 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 that the 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 Advanced Threat Prevention uses a number of deception techniques to trick the malware into determining this is a real user environment. For example, Sky Advanced Threat Prevention can:

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

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

Machine Learning Algorithm

Sky Advanced Threat Prevention 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 reprogrammed to get smarter as threats evolve.

Related Documentation

- Sky Advanced Threat Prevention Overview on page 16
- Dashboard Overview on page 25

Sky ATP Licensed Features and File Scanning Limits

Sky ATP has two service levels:

- Free
- Premium

The free model solution is available to all SRX Series customers that have a valid support contract, but it only scans executable file types. Based on this result, the SRX Series device can allow the traffic or perform inline blocking.

The premium model is available with additional licensing and provides deeper analysis. All file types are examined using several analysis techniques to give better coverage. Full reporting provides details about the threats found on your network.

NOTE: C&C and GeoIP filtering feeds are only available with a Premium license. For information on licensed features, see the table below.

The following table shows a comparison between the free model and the premium model.

Table 5: Comparing the Sky Advanced Threat Prevention Free Model and Premium Model

Free 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.
Inbound protection.	Inbound protection.
Inspects only .exe file types.	No restrictions on object file types inspected beyond those imposed by the Sky Advanced Threat Prevention service. You can specify which file types are sent to service for inspection.
Executables go through the entire pipeline (cache, antivirus, static, and dynamic).	Executables, PDF files, and Microsoft Office files (Word document, Excel, and PowerPoint) go through the entire pipeline (cache, antivirus, static, and dynamic). All other file types only go through the cache and antivirus pipeline.
—	C&C feeds.
Infected host blocking.	Infected host blocking.
—	GeoIP filtering.
Up to 2500 files per day per device submitted to cloud for inspection.	Up to 10,000 files per day per device submitted to the cloud for inspection.
Outbound protection.	Outbound protection.
—	C&C protection with event data returned to the Sky Advanced Threat Prevention Cloud.
Reporting on malware blocked (counts only; no detailed behaviors exposed).	Reporting with rich detail on malware behaviors.
—	Compromised endpoint dashboard.

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.

Table 6: File Scanning Limits

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

Related Documentation

- Sky Advanced Threat Prevention Overview on page 16
- Dashboard Overview on page 25

CHAPTER 2

Dashboard

- Dashboard Overview on page 25

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 a Premium license. For information on other licensed features, see Sky ATP Licensing.

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.

Table 7: Sky ATP Dashboard Widgets *(continued)*

Widget	Definition
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

- Sky Advanced Threat Prevention Overview on page 16
- Remediation and Malware Detection Overview on page 19
- *Sky Advanced Threat Prevention Licenses*
- Hosts Overview on page 27
- File Scanning Overview on page 30
- Command and Control Servers Overview on page 29

CHAPTER 3

Monitor

- Hosts Overview on page 27
- Host Details on page 28
- Command and Control Servers Overview on page 29
- File Scanning Overview on page 30
- File Scanning Details on page 31
- File Scanning Limits on page 32
- Manual Scanning Overview on page 33

Hosts Overview

This 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.
- Collect personal information, such as passwords and account numbers.

In Sky ATP, compromised hosts are listed as secure intelligence data feeds (also called information sources.) The data feed lists the IP address or IP subnet of the host along with a threat level; for example, 130.131.132.133 and threat level 5. Once identified, Sky Advanced Threat Prevention recommends an action and you can create security policies to take enforcement actions on the inbound and outbound traffic on these infected hosts.

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.

Related Documentation

- Host Details on page 28
- File Scanning Overview on page 30
- File Scanning Details on page 31
- Manual Scanning Overview on page 33

- Dashboard Overview on page 25

Host Details

Use this page to view detailed information about current threats to this specific host by time frame. From here you can change the investigation status and the blocked status of this host.

The information provided on the host details page is as follows:

Table 8: Threat Level Definitions

Threat Level	Definition
0	Clean; no action is required.
1–3	Low threat level. Recommendation: Disable this host.
4–6	Medium threat level. Recommendation: Disable this host.
7–10	High threat level. Host has been automatically blocked.

- Host Status—Displays the current state by threat level, which could be any of the levels described in the table above.
- Investigation Status—The following states of investigation are available: Open, In progress, Resolved - false positive, Resolved - fixed, and Resolved - ignored.
- Blocked Status—The following blocked statuses are available: Automatic, Block manually, and Allow manually.

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 27
- File Scanning Overview on page 30
- File Scanning Details on page 31
- Manual Scanning Overview on page 33
- Dashboard Overview on page 25

Command and Control Servers Overview

NOTE: C&C and GeoIP filtering feeds are only available with a premium license. For information on licensed features, see Sky ATP Licensing.

This page lists information on C&C 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 feed information from Sky Advanced Threat Prevention 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.

The following information is available on this page.

Table 9: 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.

Table 9: Command & Control Server Data Fields *(continued)*

Field	Definition
Action	Te action taken on the communication (permitted or blocked).

Related Documentation

- Host Details on page 28
- Hosts Overview on page 27
- Dashboard Overview on page 25

File Scanning Overview

Sky ATP keeps a record 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 File Scanning 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.

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 10: 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 level of the file, 0-10. See Host Details for threat level definitions.
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

- File Scanning Limits on page 32
- File Scanning Details on page 31
- Manual Scanning Overview on page 33
- Hosts Overview on page 27

- Host Details on page 28
- Dashboard Overview on page 25

File Scanning Details

Use this page to view analysis information and a malware behavior summary for the downloaded file. The following information is displayed for suspicious files.

- File Summary
- Hosts that have downloaded the file
- Malicious behavior summary

File Summary

Table 11: File Summary Fields

Field	Definition
Platform	The operating system of the host that downloaded the file. Example, Win32.
Threat 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.
Last Scanned	The time and date of the last scan to detect the suspicious file.
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe,, wordmui.msi.
File Size	The size of the downloaded file in bytes.
AV Results	If the AV scanner determines the file is a virus, this field indicates "positive." If not, the field indicates "negative."
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.

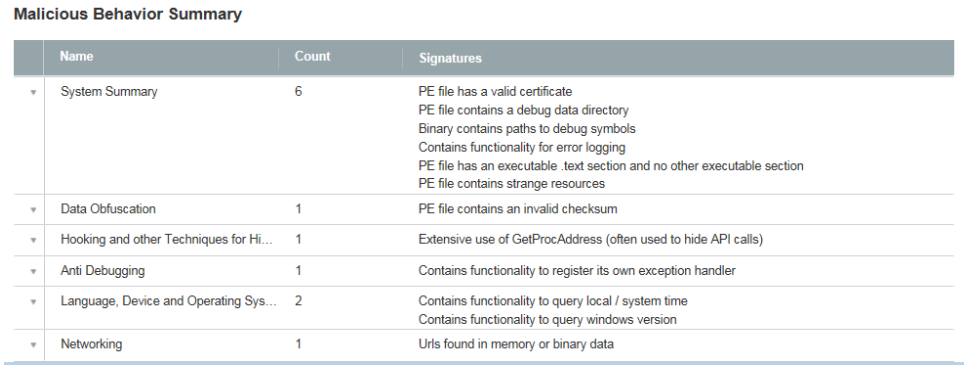
Hosts That have Downloaded the File

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.

Malware Behavior Summary

The information displayed here varies according to the malware type. Here is an example of a behavior summary for a level 10 threat.

Figure 3: Screen Capture: Malicious Behavior Summary



Malicious Behavior Summary

	Name	Count	Signatures
▾	System Summary	6	PE file has a valid certificate PE file contains a debug data directory Binary contains paths to debug symbols Contains functionality for error logging PE file has an executable .text section and no other executable section PE file contains strange resources
▾	Data Obfuscation	1	PE file contains an invalid checksum
▾	Hooking and other Techniques for Hi...	1	Extensive use of GetProcAddress (often used to hide API calls)
▾	Anti Debugging	1	Contains functionality to register its own exception handler
▾	Language, Device and Operating Sys...	2	Contains functionality to query local / system time Contains functionality to query windows version
▾	Networking	1	Urls found in memory or binary data

Related Documentation

- File Scanning Limits on page 32
- File Scanning Overview on page 30
- Manual Scanning Overview on page 33
- Hosts Overview on page 27

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.

Limit thresholds operate on a sliding scale and are calculated within 24-hour time-frame starting "now."

Table 12: File Scanning Limits

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

Related Documentation

- File Scanning Details on page 31
- Manual Scanning Overview on page 33

- Hosts Overview on page 27
- Host Details on page 28
- Dashboard Overview on page 25

Manual Scanning Overview

If you suspect a file is suspicious, you can manually upload it to Sky ATP 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.

Table 13: 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 level of the file, 0-10. See Host Details for threat level definitions.
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

- File Scanning Details on page 31
- File Scanning Overview on page 30
- Host Details on page 28

CHAPTER 4

Devices

- Enrolled Devices on page 35
- Enrolling and Disenrolling Devices on page 36
- Device Lookup Overview on page 38
- Device Information on page 38

Enrolled Devices

Only devices enrolled with Sky ATP can send files for malware inspection. This page provides basic connection information for all devices, 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.

Select a device and click one of the following buttons:

Table 14: 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 or free) of the device. For this search, the device does not have to be currently enrolled in Sky ATP.
Remove	Removing an SRX Series device is different than disenrolling it. Use the Remove option only when the associated SRX Series device is not responding (for example, hardware failure). Removing it, disassociates it from the cloud without running the Junos OS operation (op) script on the device (see "Enrolling and Disenrolling Devices" on page 36). You can later enroll it using the Enroll option when the device is again available.

Related Documentation

- Device Lookup Overview on page 38
- Enrolling and Disenrolling Devices on page 36

- Device Information on page 38

Enrolling and Disenrolling Devices

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**. Your screen will look similar to the following:

```
root@mysystem> op url http://skyatp.argon.junipersecurity.net/bootstrap/
enroll/6e797dc797d26129dae46f17a7255650/jpz1qkddodlcav5g.slax

ersion JUNOS Software Release [15.1-X49] is valid for bootstrapping.

Going to enroll single device for SRX1500: P1C_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!
```

The SRX Series device you enrolled now appears in devices list.

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

4. (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.

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 disasssociate 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. Your screen will look similar to the following.

```
root@mysystem> op url http://skyatp.argon.junipersecurity.net/bootstrap/
disenroll/6e797dc797d26129dae46f17a7255650/jpz1qkddodlcav5g.slax

oing to disenroll single device for SRX1500: P1C_00000067...

Communicate with cloud...

P1C_00000067 disenrolled...

Clear CA profile aamw-ca...

Clear CA profile aamw-cloud-ca...

Clear CA profile aamw-secintel-ca...

Clear local certificate aamw-srx-cert with CA server...
```

```
Clear key pair: aamw-srx-cert...

Remove advanced-anti-malware services...

Restart aamwd...

Wait for aamwd connection status #1...

SRX was disenrolled successfully!
```

The device is no longer enrolled with the cloud and is removed from the Web UI Devices table.

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

Related Documentation

- Enrolled Devices on page 35
- Device Lookup Overview on page 38
- Device Information on page 38

Device Lookup Overview

Using the Device Lookup wizard, you can search for any SRX Series device enrolled within your Sky ATP security realm. This option provides another way to see if a device is using the free license or a premium license.

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 this search, the device does not have to be currently enrolled in Sky ATP.

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

Once located, the serial number, model number, and tier are displayed for the listed devices.

NOTE: **All serial numbers you enter must be valid. Otherwise, the results will be empty for all entries.**

Related Documentation

- Enrolled Devices on page 35
- Enrolling and Disenrolling Devices on page 36
- Device Information on page 38

Device Information

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

Table 15: Device Information Fields

Field	Definition
Device Information	
OS Version	SRX Series device JunOS version
Model Number	SRX Series device model number
Serial Number	SRX Series device serial number
Device Name	SRX Series device
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	
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

- Device Lookup Overview on page 38
- Enrolling and Disenrolling Devices on page 36
- Enrolled Devices on page 35

CHAPTER 5

Configure

- Custom Whitelist and Blacklist Overview on page 41
- Creating Whitelists and Blacklists on page 42
- Device Profiles Overview on page 43
- Creating Device Profiles on page 44

Custom 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.

Related Documentation

- Creating Whitelists and Blacklists on page 42
- File Scanning Overview on page 30
- File Scanning Details on page 31
- Hosts Overview on page 27
- Host Details on page 28

Creating Whitelists and 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.

Before You Begin

- Read the "Custom Whitelist and Blacklist Overview" on page 41 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.

Configuring Whitelists and Blacklists

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 Table 16 on page 42 below.

3. Click **OK**.

Table 16: Whitelist and Blacklist: Domain, IP, and URL Required Information and Syntax

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

- Custom Whitelist and Blacklist Overview on page 41
- File Scanning Overview on page 30
- File Scanning Details on page 31
- Hosts Overview on page 27
- Host Details on page 28

Device Profiles Overview

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 17: File Category Contents

Category	Description	Included File Types
Active media	Flash and Silverlight applications	.swf, .xap, .xbap
Archive	Archive files	.7z, .bz2, .cab, .gz, .iso, .lz, .lzma, .ova, .rar, .s7z, .tar, .tar.gz, .tar.lzma .tbz, .tgz, .z, .zip, tar.bz2
Code	Source code	.c, .cc, .cpp, .cxx, .h, .htt, .java
Config	Configuration files	.inf, .ini, .lnk, .reg, .plist
Document	All document types except PDFs	.chm, .doc, .docx, .dotx, .hta, .html, .pot, .ppa, .pps, .ppt, .pptsm, .pptx, .ps, .rtf, .rtf, .txt, .xlsx, .xml, .xsl, .xslt
Emerging threat	A special category that includes known threat source file types	
Executable	Executable binaries	.bin, .com, .dat, .exe, .msi, .msm, .mst
Java	Java applications, archives, and libraries	.class, .ear, .jar, .war
Library	Dynamic and static libraries and kernel modules	.a, .dll, .kext, .ko, .o, .so, ocx
Media	Audio video formats	.asf, .wmv
Mobile	Mobile applications for iOS and Android	.apk, .ipa
OS package	OS-specific update applications	.deb, .dmg, .deb

Table 17: File Category Contents *(continued)*

Category	Description	Included File Types
Script	Scripting files	.bat, .js, .pl, .ps1, .py, .sct .sh, .tcl, .vbs, plsm, pyc, pyo
Portable document	PDF, e-mail, and MBOX files	.email, .mbox, .pdf, .pdfa

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 model of Sky ATP, you are limited to only the executable file category.

Related Documentation

- Creating Device Profiles on page 44
- Enrolled Devices on page 35
- Enrolling and Disenrolling Devices on page 36

Creating Device 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.

Before You Begin

- Review the "Device Profiles Overview" on page 43 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 model of Sky Advanced Threat Prevention, you are limited to only the executable file category.

Configuring Device Profiles

To create a device profile:

1. Select **Configure** > **Device Profiles**.

2. Click the plus sign (+). Complete the configuration according to the guidelines provided in the Table 18 on page 45 below.
3. Click **OK**.

Table 18: 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	Select the check boxes beside the file categories you want to send to the cloud for inspection.
Maximum File Size	(Optional) Set the maximum file size, in megabytes, for the selected file categories. 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.

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.

To edit an existing device profile:

1. Select the profile to edit from the list and click the pencil icon.
2. Make your necessary changes and click **OK**.

To delete an existing device profile, select it from the list and click the **X** icon.

Related Documentation

- Device Profiles Overview on page 43
- Enrolled Devices on page 35
- Enrolling and Disenrolling Devices on page 36

CHAPTER 6

Administration

- Modifying My Profile on page 47
- User Profiles Overview on page 48
- Creating and Editing User Profiles on page 48
- Global Configuration Overview on page 49
- Creating and Editing Global Configurations on page 49

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.

Before You Begin

- Note that your username must be a valid e-mail address.
- If you are changing your password, make sure you understand the syntax requirements.

Editing Your Profile

NOTE: **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 the **Administration** tab. This takes you to the My Profile landing page.
2. Edit the following fields. See Table 19 on page 48 below.
3. Click **OK** to save your changes or click **Reset** to discard them.

To change only your password, click **Change Password**.

Table 19: My Profile Fields

Setting	Guideline
First Name	Enter a string beginning with an an alphanumeric character.
Last Name	Enter a string beginning with an an alphanumeric character.
E-mail	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

- User Profiles Overview on page 48
- Creating and Editing User Profiles on page 48
- Global Configuration Overview on page 49

User Profiles Overview

This page provides a list of all administrator usernames and e-mail addresses. Multiple administrators can log in to the Web UI at the same time. The Web UI does not lock windows when someone is editing it, nor does it notify other sessions that a person is using it. 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.

Related Documentation

- Creating and Editing User Profiles on page 48
- Modifying My Profile on page 47
- Global Configuration Overview on page 49

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.

Before You Begin

- Review the "Modifying My Profile" on page 47 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.

Configuring User Profiles

To add additional administrator accounts:

1. Select **Administration** > **Users**.

2. Enter the information described in Table 20 on page 49 below.
3. Click **OK**.

Table 20: 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

- User Profiles Overview on page 48
- Modifying My Profile on page 47
- Global Configuration Overview on page 49

Global 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.

Related Documentation

- Creating and Editing Global Configurations on page 49
- Creating and Editing User Profiles on page 48
- User Profiles Overview on page 48
- Modifying My Profile on page 47

Creating and Editing Global Configurations

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

Before You Begin

- Review the "Global Configuration Overview" on page 49 topic.

- Decide which users will receive notifications. It might not be necessary for all users to receive alerts.

Configuring Global Settings

To create or update the global settings:

1. Select **Administration** > **Global Configuration**.
2. (Premium licenses only) Set the default threat level threshold.
3. Click the plus sign to create e-mail alerts, or click the pencil icon to edit existing ones. Configure the fields described in Table 21 on page 50 below.
4. Click **OK**.

Table 21: 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 Configuration Overview on page 49
- User Profiles Overview on page 48
- Modifying My Profile on page 47

CHAPTER 7

More information

- Links to Documentation on Juniper.net on page 51

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, refer to the Sky Advanced Threat Prevention Administration 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.

CHAPTER 8

Index

- Index on page 55

Index

Symbols

#, comments in configuration statements....xi
( ), in syntax descriptions....xi
< >, in syntax descriptions....xi
[ ], in configuration statements....xi
{ }, in configuration statements....xi
| (pipe), in syntax descriptions....xi

B

braces, in configuration statements....xi
brackets
    angle, in syntax descriptions....xi
    square, in configuration statements....xi

C

comments, in configuration statements....xi
conventions
    text and syntax....x
curly braces, in configuration statements....xi
customer support....xii
    contacting JTAC....xii

D

documentation
    comments on....xi

F

font conventions....x

M

manuals
    comments on....xi

P

parentheses, in syntax descriptions....xi

S

support, technical *See* technical support
syntax conventions....x

T

technical support
    contacting JTAC....xii