Juniper Networks | Engineering Simplicity

Juniper Advanced Threat Prevention Cloud

Juniper ATP Cloud User Guide

Published
2026-02-05

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

Juniper Advanced Threat Prevention Cloud Juniper ATP Cloud User 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 https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to configure and monitor Juniper Advanced Threat Prevention (ATP) Cloud features from the ATP Cloud portal to protect all hosts in your network against evolving security threats.

1

PART

Introduction

CHAPTER 1

Juniper Advanced Threat Prevention Cloud Overview

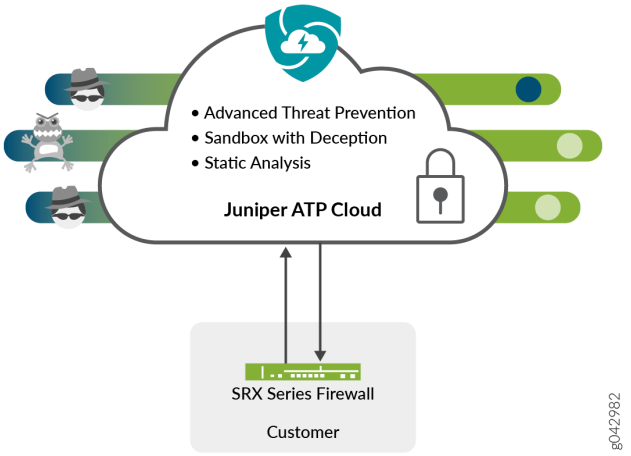
IN THIS CHAPTER

About Juniper ATP Cloud

IN THIS SECTION

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

Figure 1: Juniper ATP Cloud Overview



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

- The SRX Series Firewall 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 Firewall blocks known malicious file downloads and outbound C&C traffic.

Juniper ATP Cloud supports the following modes:

- Layer 3 (L3) mode
- Tap mode
- Transparent mode using MAC address

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

Juniper ATP Cloud Features

Juniper ATP Cloud is a cloud-based solution. Cloud environments are flexible and scalable, and a shared environment ensures that everyone benefits from new threat intelligence in near real-time. Your

sensitive data is secured even though it is in a cloud shared environment. Security analysts can update their defense when new attack techniques are discovered and distribute the threat intelligence with very little delay.

In addition, Juniper ATP Cloud offers the following features:

- Integrated with the SRX Series Firewall 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
- AI-Predictive Threat Prevention, an intelligent and fast malware detection and prevention solution, protects your network wherever users connect from. This solution leverages flow-based antivirus and machine learning-based zero-day threat detection to protect users from malware attacks and to prevent spreading of malware in your system. See Configure Flow-Based Antivirus Policy and Configure Machine Learning-Based Threat Detection.
- 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
- API for C&C feeds, allowlist and blocklist operations, and file submission. See the Threat Intelligence Open API Setup Guide for more information.
- Domain Name System (DNS), Encrypted Traffic Insights (ETI) and Internet of Things (IoT) security. For licensing information specific to these features, see Software Licenses for ATP Cloud.

Figure 2 on page 5 lists the Juniper ATP Cloud components.

Figure 2: Juniper ATP Cloud Components

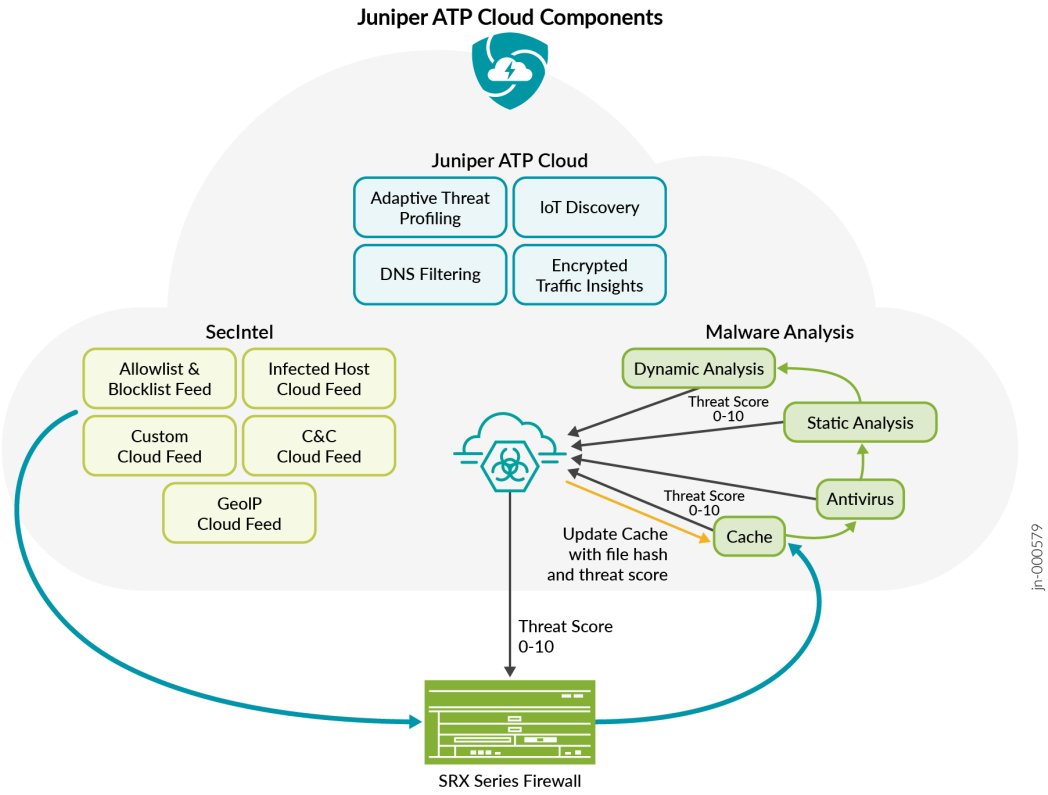


Table 1 on page 5 briefly describes each Juniper ATP Cloud component's operation.

Table 1: Juniper ATP Cloud Components

Component	Operation
C&C cloud feeds	C&C feeds are essentially a list of servers that are known C&C 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.

Table 1: Juniper ATP Cloud Components *(Continued)*

Component	Operation
Allowlist, blocklists and custom cloud feeds	An allowlist is simply a list of known IP addresses that you trust and a blocklist is a list that you do not trust.
SRX Series Firewall	Submits extracted file content for analysis and detected C&C hits inside the customer network. Performs inline blocking based on file signature database provided by Juniper ATP Cloud.
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 refine which file categories can be submitted into the cloud for processing.
Encrypted Traffic Insights	Encrypted Traffic Insights restores visibility lost due to encrypted traffic without the heavy burden of full TLS/SSL decryption.
SecIntel	Provides curated SecIntel in the form of threat feeds that include malicious domains, URLs, and IP addresses used in known attack campaigns. SecIntel also enables customers to feed and distribute their own threat intelligence for inline blocking.
Adaptive Threat Profiling	Automatically create SecIntel threat feeds based on who and what is currently attacking the network to combat the continuous onslaught of new threats. Adaptive Threat Profiling leverages Juniper Security Services to classify endpoint behavior and build custom threat intelligence feeds that can be used for further inspection or blocking at multiple enforcement points.

Table 1: Juniper ATP Cloud Components *(Continued)*

Component	Operation
DNS Security	Provides threat prevention from attacks that utilize DGA and DNS tunneling techniques. Protect against DNS exploits for C&C communications, data exfiltration, phishing attacks, and ransomware that commonly exploit DNS using a variety of techniques.
IoT Threat Prevention	ATP Cloud allows customers to control the IoT attack surface on their network by providing an easy way to identify and categorize the IoT devices

How the SRX Series Firewall Remediates Traffic

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

For inbound traffic, security policies on the SRX Series Firewall look for specific types of files, like .exe files, to inspect. When one is encountered, the security policy sends the file to the Juniper ATP Cloud cloud for inspection. The SRX Series Firewall holds the last few KB of the file from the destination client while Juniper ATP Cloud checks if this file has already been analyzed. If so, a verdict is returned and the file is either sent to the client or blocked depending on the file's threat level and the user-defined policy in place. If the cloud has not inspected this file before, the file is sent to the client while Juniper ATP Cloud 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?.

Figure 3 on page 8 shows an example flow of a client requesting a file download with Juniper ATP Cloud.

Figure 3: Inspecting Inbound Files for Malware

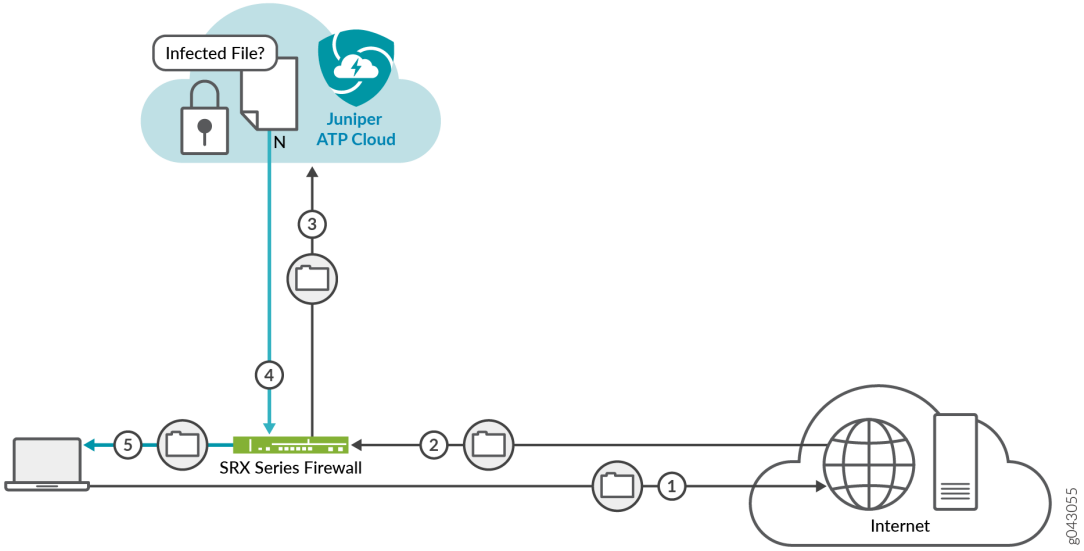


Table 2: Malware Inspection Workflow

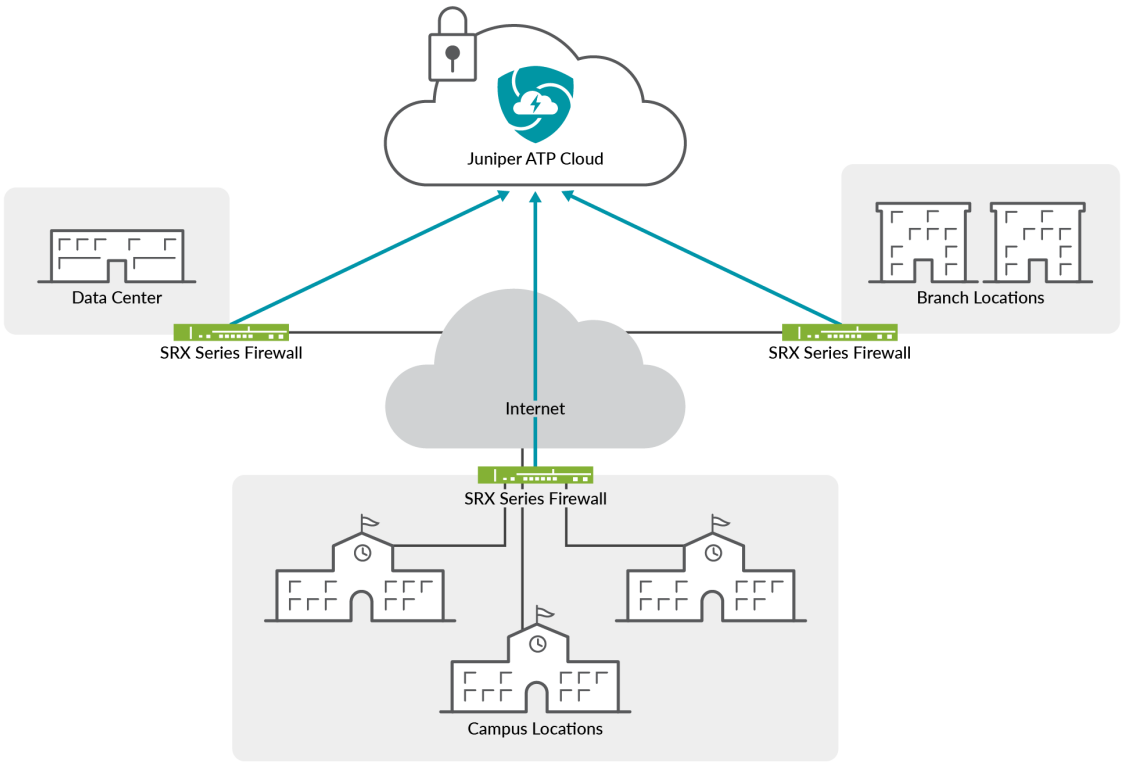
Step	Description
1	A client system behind an SRX Series Firewalls requests a file download from the Internet. The SRX Series Firewall forwards that request to the appropriate server.
2	The SRX Series Firewall receives the downloaded file and checks its security profile to see if any additional action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

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

Juniper ATP Cloud Use Cases

Juniper ATP Cloud can be used anywhere in an SRX Series deployment. See Figure 4 on page 9

Figure 4: Juniper ATP Cloud Use Cases



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

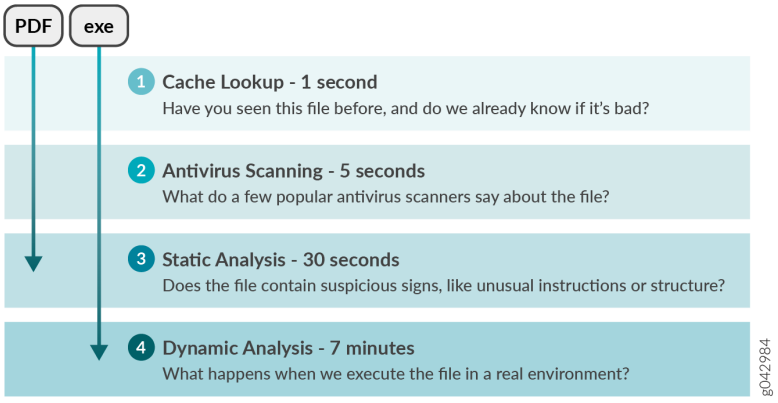
How Is Malware Analyzed and Detected?

IN THIS SECTION

Analyze and Detect Malware

Juniper ATP Cloud 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 10.

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



Each analysis technique creates a verdict number, which is combined to create a final verdict number between 0 and 10. A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series Firewall compares this verdict number to the policy settings and either

permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.

Cache Lookup

When a file is analyzed, a file hash is generated, and the results of the analysis are stored in a database. When a file is uploaded to the Juniper 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 Firewall and there is no need to re-analyze the file. In addition to files scanned by Juniper ATP Cloud, information about common malware files is also stored to provide faster response.

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

Antivirus Scan

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

Juniper ATP Cloud utilizes multiple antivirus software packages, not just one, to analyze a file. The results are then fed into the machine learning (ML) 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 ML 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 OS environment is set up, typically in a VM, 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 ML algorithm to generate a verdict.

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

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.

ML Algorithm

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

Threat Levels

Juniper ATP Cloud 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 3 on page 12.

Table 3: Threat Level Definitions

Threat Level	Definition
0	Clean; no action is required.

Table 3: Threat Level Definitions *(Continued)*

Threat Level	Definition
1 - 3	Low threat level.
4 - 6	Medium threat level.
7 -10	High threat level.

For more information about threat levels, see the Juniper ATP Cloud Web UI online help.

RELATED DOCUMENTATION

About Juniper ATP Cloud | 2

Dashboard Overview | 44

About Policy Enforcer

IN THIS SECTION

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/content/dam/www/assets/datasheets/us/en/security/policy-enforcer-datasheet.pdf

Policy Enforcer provides centralized, integrated management of all your security devices (both physical and virtual), giving you the ability to combine threat intelligence from different solutions and act on that intelligence from one management point.

It also automates the enforcement of security policies across the network and quarantines infected endpoints to prevent threats across firewalls and switches. It works with cloud-based Juniper ATP Cloud

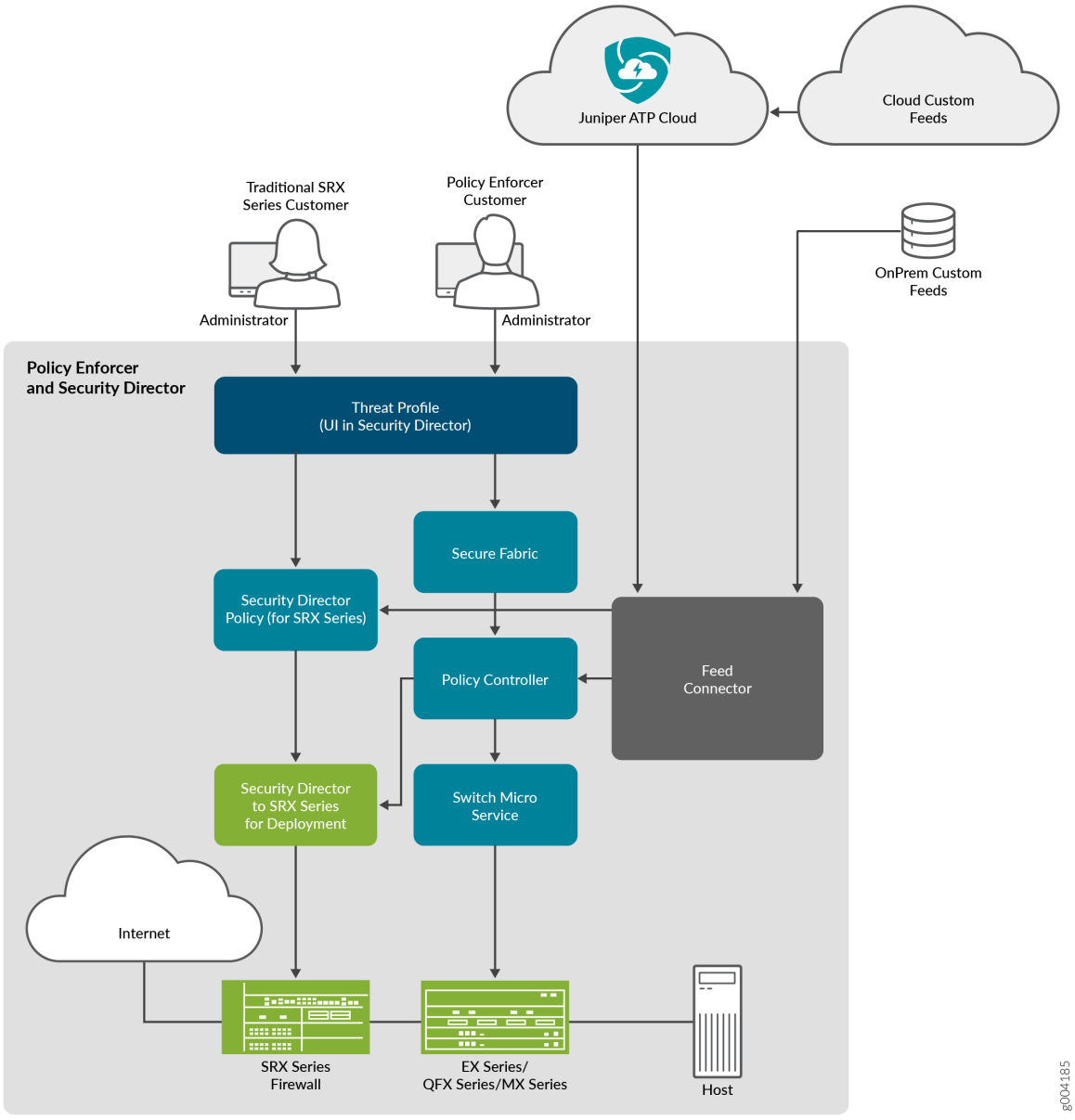
to protect both perimeter-oriented threats as well as threats within the network. For example, if a user downloads a file from the Internet and that file passes through an SRX Series Firewall, the file can be sent to the Juniper ATP Cloud cloud for malware inspection (depending on your configuration 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 15 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 | 75

Host Details | 79

Dashboard Overview | 44

CHAPTER 2

Juniper Advanced Threat Cloud Prevention Setup

IN THIS CHAPTER

Onboarding Overview

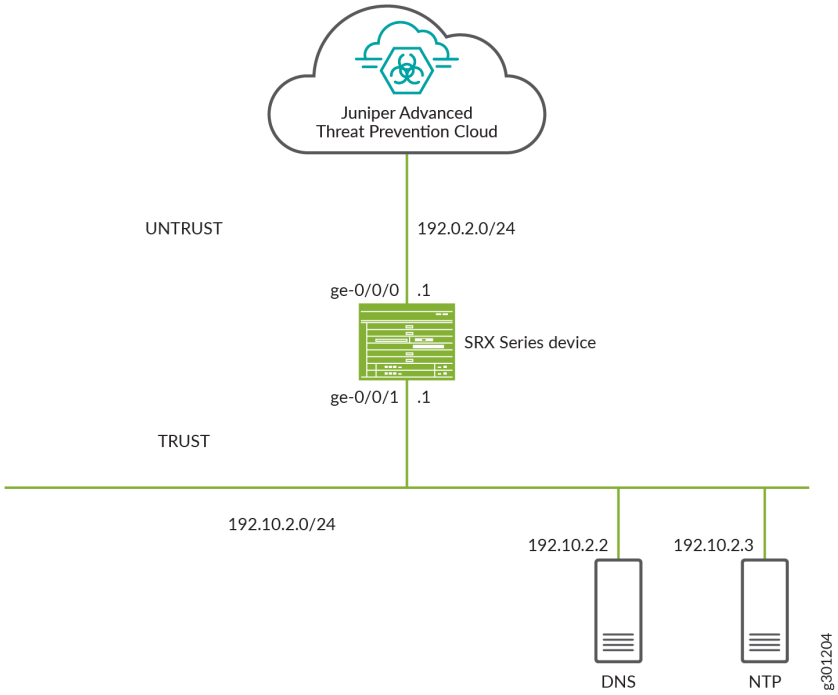
SUMMARY

This topic walks you through the essential steps for getting started with Juniper ATP Cloud. You can perform key tasks needed to set up your account, configure core services, and prepare your environment so you can begin using ATP Cloud effectively.

IN THIS SECTION

Juniper ATP Cloud Topology

Here's an example of how you can deploy Juniper ATP Cloud to protect a host in your network against security threats.



Get Your Juniper ATP Cloud License

You'll need to get your Juniper ATP Cloud license before you can start configuring Juniper ATP Cloud on your SRX Series Firewall. Contact your local sales office or Juniper Networks partner to place an order for a Juniper ATP Cloud license. Once the order is complete, an activation code is sent to you by email. You'll use this code with your SRX Series Firewall serial number to generate a license entitlement. Use the `show chassis hardware` CLI command to find the serial number of the SRX Series Firewall.

To know about Juniper ATP Cloud licenses, see Software Licenses for ATP Cloud. For further details, see the product Data Sheets or contact your Juniper Account Team or Juniper Partner.

To obtain the license:

1. Go to https://license.juniper.net and log in with your Juniper Networks Customer Support Center (CSC) credentials.
2. Select **SRX Series Devices** or **vSRX** from the Generate Licenses list.
3. Using your authorization code and SRX Series serial number, follow the instructions to generate your license key.
    - If you are using Juniper ATP Cloud with SRX Series Firewalls, then you don't need to enter the license key because it is automatically transferred to the cloud server. It can take up to 24 hours for your license to be activated.

- If you are using Juniper ATP Cloud with vSRX Virtual Firewall, the license is not automatically transferred. You'll need to install the license. For more details, see Software Licenses for vSRX Virtual Firewall. After the license is generated and applied to a specific vSRX Virtual Firewall, use the `show system license` CLI command to view the software serial number of the device.

Congratulations! You have successfully activated your Juniper ATP Cloud license.

WHAT's NEXT

- "Register a Juniper ATP Cloud Account" on page 22
- "Download And Run the Juniper ATP Cloud Script" on page 26
- "Enroll an SRX Series Firewall Using Juniper ATP Cloud Web Portal" on page 51
- "Enroll an SRX Series Firewall in Juniper ATP Cloud Using J-Web" on page 55

Manage the Juniper ATP Cloud License

IN THIS SECTION

This topic describes how to install the Juniper ATP Cloud license onto your SRX Series Firewalls and vSRX deployments. For more information, see Software Licenses for ATP Cloud.

When installing the license key, you must use the license that is specific your device type.

Obtaining the License Key

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

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

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

2. (SRX Series Firewalls only) Use the `show chassis hardware` CLI command to find the serial number of the SRX Series Firewalls that are to be tied to the Juniper ATP Cloud license.

```
run show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                CM1915AK0326      SRX1500
Midplane         REV 09   750-058562   ACMH1590          SRX1500
Pseudo CB 0
Routing Engine 0          BUILTIN      BUILTIN           SRX Routing Engine
FPC 0            REV 08   711-053832   ACMG3280          FEB
  PIC 0                   BUILTIN      BUILTIN           12x1G-T-4x1G-SFP-4x10G
```

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

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

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

License Management and SRX Series Firewalls

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

Juniper ATP Cloud Premium Trial License for vSRX Virtual Firewall

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

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

> **NOTE**: The 30-day trial license period begins on the day you install the evaluation license.
>
> To continue using Juniper ATP Cloud 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 organization and contact information before using Juniper ATP Cloud. For more information, see Register a Juniper Advanced Threat Prevention Cloud Account.

License Management and vSRX Virtual Firewall Deployments

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

The following instructions describe how to install a license key from the CLI. You can also add a new license key with J-Web. See Managing Licenses for vSRX.

> **NOTE**: If you are reinstalling a Juniper ATP Cloud license key on your vSRX, you must first remove the existing Juniper ATP Cloud license. For information about 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.

```
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 Virtual Firewall 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.

   Examples of license outputs:

```
show system license

  License identifier: JUNOS123456
  License version: 4
  Software Serial Number: 1234567890
  Customer ID: JuniperTest
  Features:
    ATP Cloud          - Cloud Based Advanced Threat Prevention on SRX firewalls
      date-based, 2016-07-19 17:00:00 PDT - 2016-07-30 17:00:00 PDT
```

```
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 Virtual Firewall.

High Availability

Before enrolling your devices with the Juniper ATP Cloud, set up your High Availability (HA) cluster as described in your product documentation. For vSRX Virtual Firewall deployments in HA configurations, each vSRX must be licensed and entitled separately. Additionally, the SSRN number of the premium license key that's added on the vSRX HA pair appears in the Enrolled Devices page in Juniper ATP Cloud. When enrolling your devices, you need to enroll it on the primary node, only. The Juniper ATP Cloud will recognize that this is a HA cluster and will automatically enroll both nodes.

Register a Juniper ATP Cloud Account

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

When setting up your Juniper ATP Cloud account, you must come up with an organization 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 organization name. Organization names can only contain alphanumeric characters and the dash (“-”) symbol.

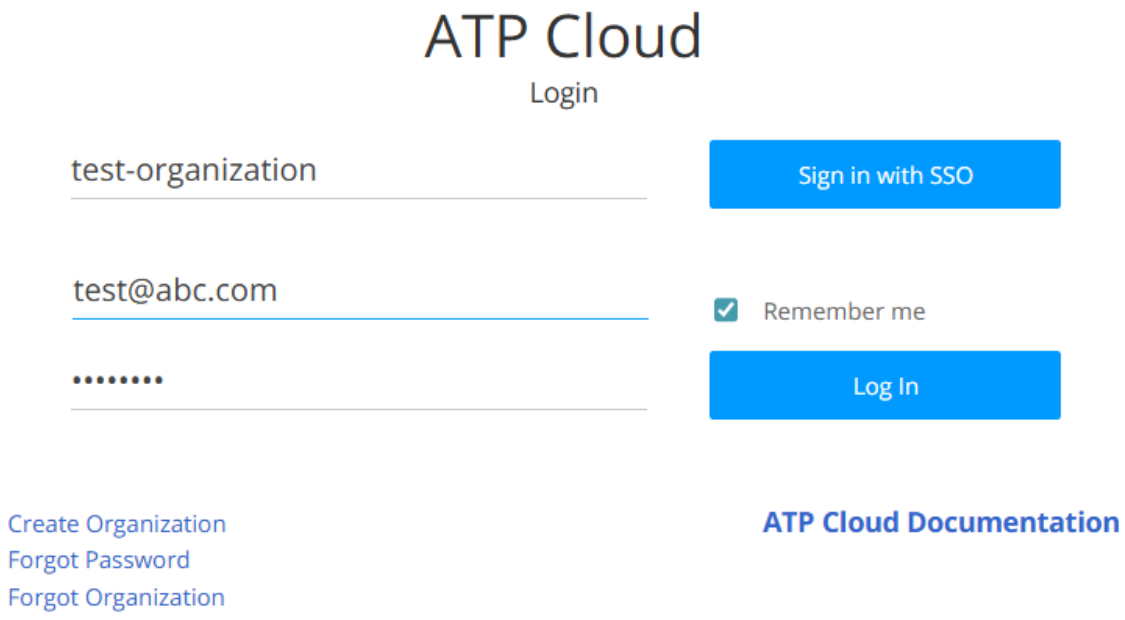
To create a Juniper ATP Cloud administrator account:

1. Open a browser, type your location specific URL and press **Enter**. See "Juniper ATP Cloud Web UI Overview" on page 38 for all portal hostnames by location.

   `https://amer.sky.junipersecurity.net`

   The management interface login page appears. See Figure 7 on page 22.

Figure 7: Juniper ATP Cloud Login



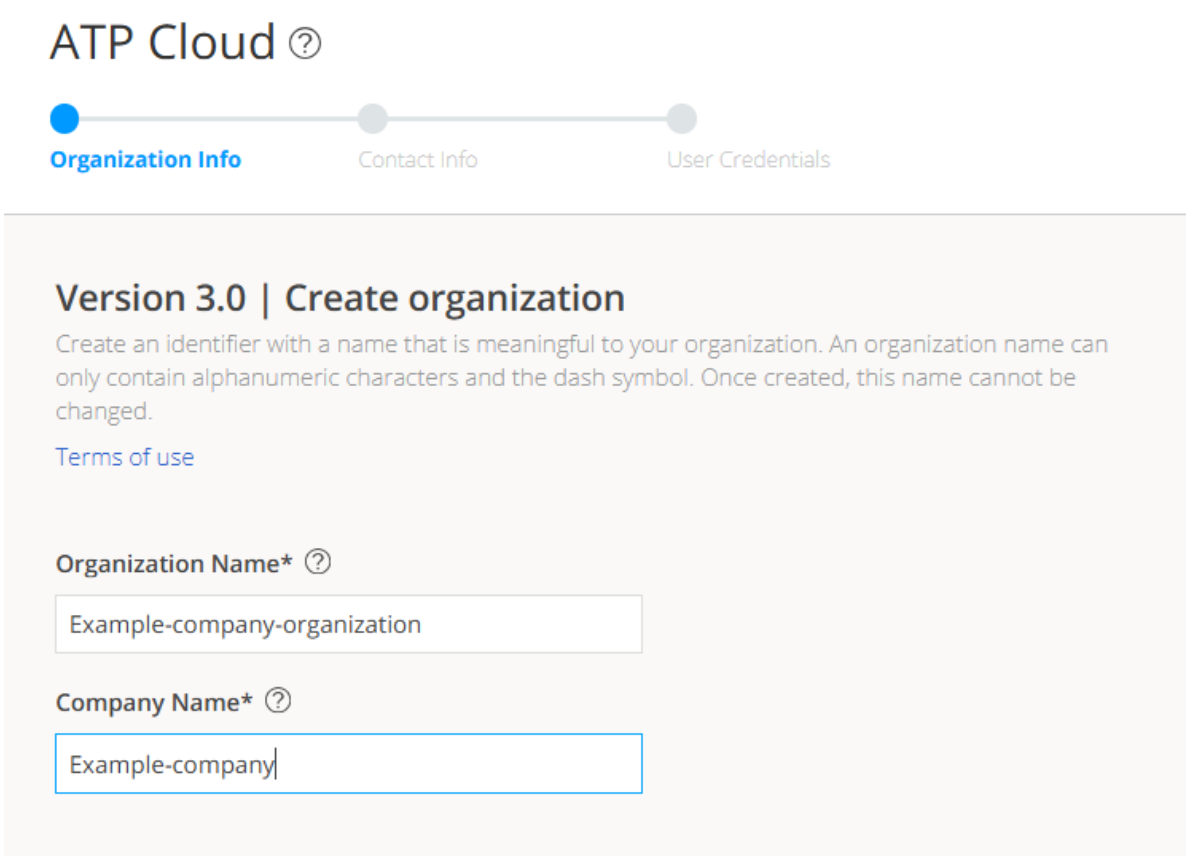
2. Click **Create Organization**.

   The authentication window is displayed.

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

The Create Organization window is displayed. See Figure 8 on page 23.

Figure 8: Create Your Juniper ATP Cloud Organization

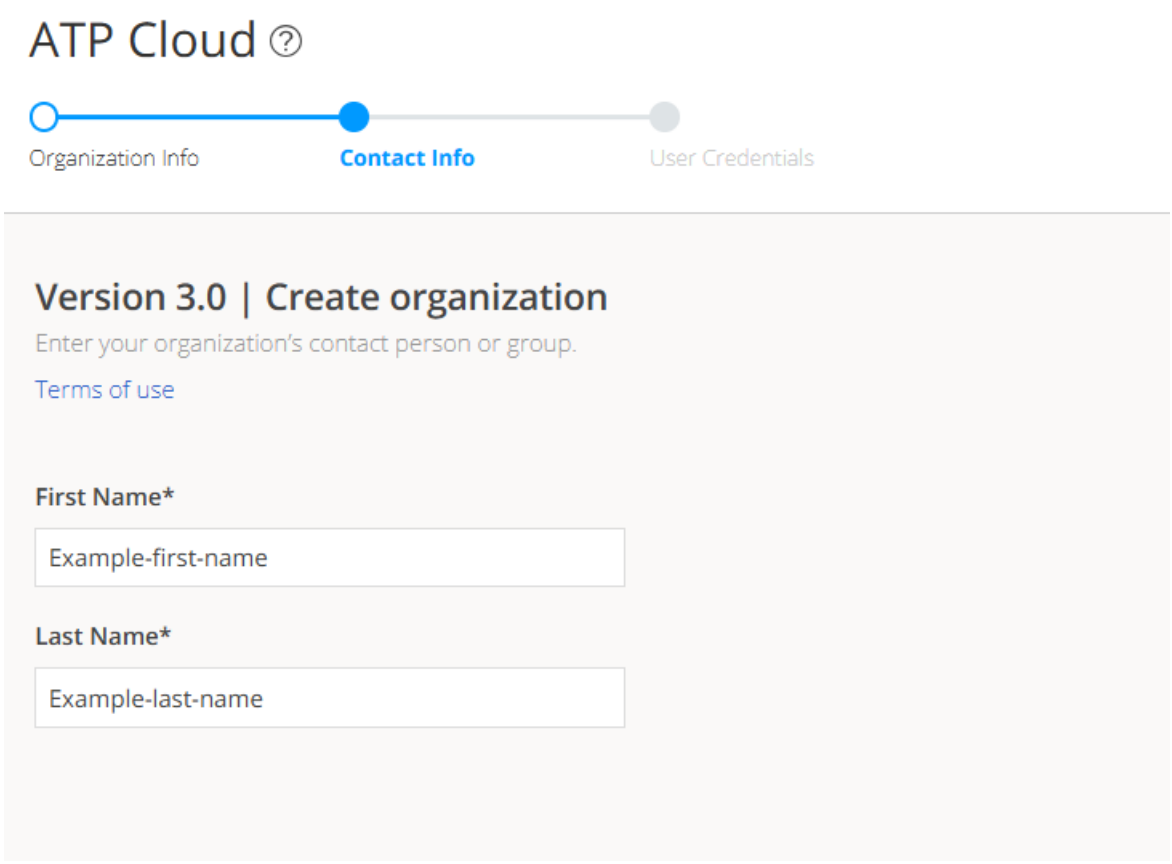


4. Enter your unique organization name and company name. Click **Next**.

> **NOTE**: Verify your organization name before you click Next. You cannot delete organizations through the Web UI.

The contact information window is displayed. See Figure 9 on page 24.

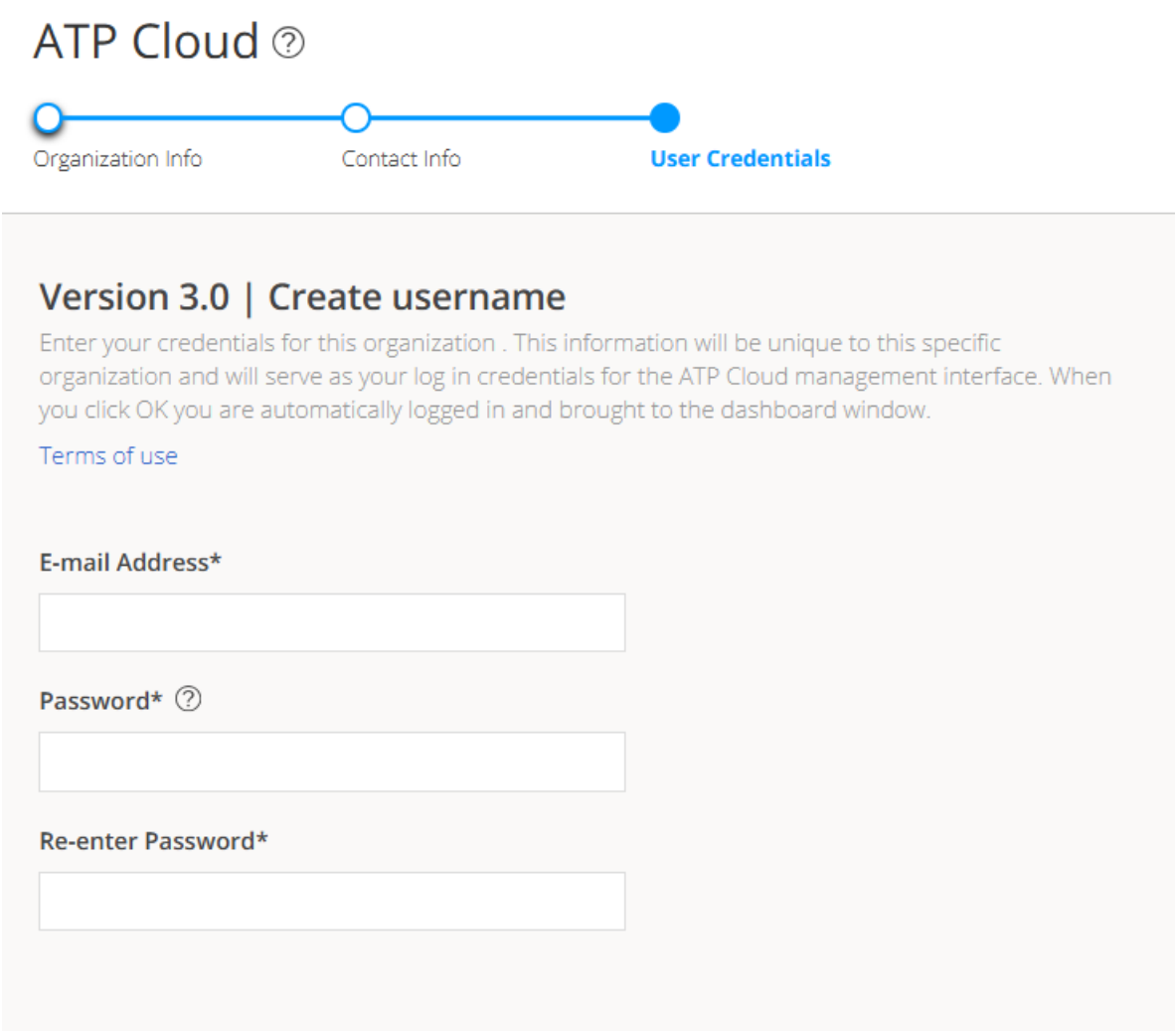
Figure 9: Entering Your Juniper ATP Cloud Contact Information



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 is displayed. See Figure 10 on page 25.

Figure 10: Creating Your Juniper ATP Cloud Credentials



6. Enter a valid e-mail address and password. This will be your log in information to access the Juniper ATP Cloud 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 an account on a new organization and re-enroll your devices.
- Contact Juniper Technical Support to reset your password.

RELATED DOCUMENTATION

Enroll an SRX Series Firewall Using the CLI

Download And Run the Juniper ATP Cloud Script

The Juniper ATP Cloud uses a Junos OS op script to help you configure your SRX Series Firewall to connect to the Juniper ATP Cloud cloud service. This script performs the following tasks:

- Downloads and installs certificate authority (CAs) licenses onto your SRX Series Firewall.

  NOTE:

  - You must allow traffic to the junipersecurity.net domain on ports 8444 and 7444 since the Trusted Platform Module (TPM)-based certificates are used for connections between the SRX Series Firewall and Juniper ATP Cloud. To determine if a feature is supported by a specific platform or Junos OS release, see Feature Explorer. For more information about using TPM on SRX Series Firewalls, see Trusted Platform Module Overview.
  - For newly enrolled TPM and non-TPM-based devices, traffic must be allowed to the junipersecurity.net domain only on port 443.

- Creates local certificates and enrolls these certificates with the cloud server
- Performs basic Juniper ATP Cloud configuration on the SRX Series Firewall
- Establishes a secure connection to the cloud server

NOTE:

- Juniper ATP Cloud requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) can connect to the Internet.
- The data plane connection should not be sourced from the management or loopback interface, such as fxp0 or lo0. You do not need to open any ports on the SRX Series Firewall to communicate with the cloud server. However, if you have a device in the middle, such as a firewall, then that device must have port 443 open.
- The SRX Series Firewall uses the default inet.0 routing table and an interface part of inet.0 as source-interface for control-plane connection from SRX Series Firewall to Juniper ATP Cloud. If the only Internet-facing interface on SRX Series Firewall is part of a routing instance, then we recommend that you add a static route pointing to the routing instance. Else, the control connection will fail to establish.

- Juniper ATP Cloud requires that your SRX Series Firewall hostname contains only alphanumeric ASCII characters (a-z, A-Z, 0-9), the underscore symbol (_) and the dash symbol (-).

For SRX300, SRX320, SRX340, SRX345, SRX380 and SRX550 Series firewalls, you must run the `set security forwarding-process enhanced-services-mode` command and reboot the device before running the op script or before running the `request services advanced-anti-malware enroll` command.

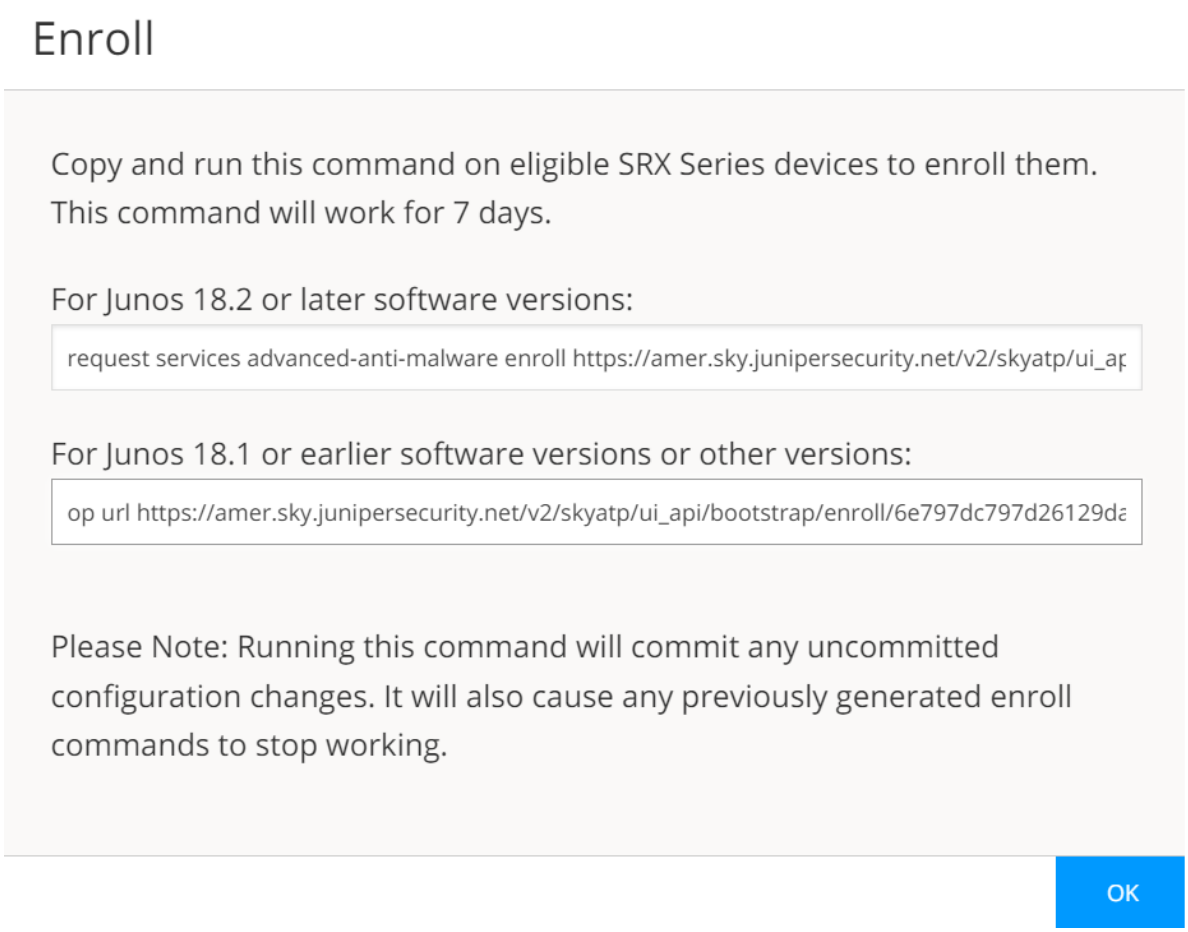
To download and run the Juniper ATP Cloud scripts:

NOTE: Starting in Junos OS Release 19.3R1, you can use the `request services advanced-anti-malware enroll` command on the SRX Series Firewall to enroll a device to the Juniper ATP Cloud Web Portal. With this command, you do not have to perform any enrollment tasks on the Web Portal. All enrollment is done from the CLI on the SRX Series Firewall. See Enroll an SRX Series Firewall Using the CLI.

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

   The Enroll window appears. See Figure 11 on page 28.

Figure 11: Enrolling Your SRX Series Firewall



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

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

3. Paste this command into the Junos OS CLI of the SRX Series Firewall you want to enroll with Juniper ATP Cloud. Press **Enter**. Your screen will look similar to the following for TPM-based and non-TPM-based devices:

   - Script for TPM-based devices:

```
request services advanced-anti-malware enroll https://amer.sky.junipersecurity.net/v2/
skyatp/ui_api/bootstrap/enroll/mt8zlb8xwl0vmg5x/8tajwglnz54sdhkn.slax
```

```
Platform is supported by ATP Cloud: SRX2300.
Version 25.4I-20250731.0.1357 is valid for bootstrapping.
Junos version 25.4I-20250731.0.1357 supports https endpoints.
Image Version: 25.4I-20250731.0.1357...
TPM supported device detected.
Junos version 25.4I-20250731.0.1357 supports TPM.
Going to enroll single device for SRX2300: <device_SSRN> with hostname <device_name>.
Application Signature DB version on this device is: 3825 (Minor). Using latest version of
Application Signature DB is recommended.
Remove related security-intelligence service configurations...
Remove related advanced-anti-malware service configurations...
Remove related SSL service configurations...
Remove related PKI configurations...
Clear local certificate aamw-srx-cert...
Clear key pair: aamw-srx-cert...
Clear CA profile aamw-cloud-ca...
Clear CA profile aamw-secintel-ca...
Building aws certificates...
Configure aws CA...
Load aws CA...
Communicate with cloud...
License type for this device: premium.
License of your device will expire in 310 days.
Configuration added successfully for SSL crypto hardware.
Configure CA aamw-ca...
Request aamw-secintel-ca CA...
Wait aamw-secintel-ca CA download status...
Load aamw-secintel-ca CA...
Request aamw-cloud-ca CA...
Wait aamw-cloud-ca CA download status...
Load aamw-cloud-ca CA...
CA certificate ready: aamw-cloud-ca...
CA certificate ready: aamw-secintel-ca...
Configure SSL service...
Configuration added successfully for SSL service.
Configure advanced-anti-malware service...
Configuration added successfully for advanced-anti-malware service.
Configure security-intelligence service...
Configuration added successfully for security-intelligence service.
Check configuration on device...
SSL profile:                          [OK]
SecIntel CA:                          [OK]
Cloud CA:                             [OK]
```

```
TPM:                                [OK]
Client cert found:                  [OK]
SSL profile action:                 [OK]
URL for advanced-anti-malware:      [OK]
Profile for advanced-anti-malware:  [OK]
URL for security-intelligence:      [OK]
Profile for security-intelligence:  [OK]
All configurations are correct for enrollment.
Communicate with cloud...
Wait for aamw connection status...
Device enrolled successfully!
Please see following links for more information:
ATP Cloud sample config:
https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/example/
configuration/sky-atp-policy-creating-cli.html
ATP Cloud quick start guide:
http://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-
products/topic-collections/sky-atp-qsg.pdf
ATP Cloud technical documents:
http://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-
products/pathway-pages/index.html
It is recommended to run diagnostic process with the following cli command to make sure
all configurations are valid:
request services advanced-anti-malware diagnostics srxapi.preprod.sky.junipersecurity.net
detail
```

This script performs the following series of checks and configurations to ensure connectivity with Juniper ATP Cloud:

a. Detect if the SRX Series Firewall is a TPM-supported platform

b. Verify whether the Junos OS version supports HTTPS endpoints

c. Identify the device type (standalone or chassis cluster)

d. Remove any existing configuration related to Juniper ATP Cloud enrollment on SecIntel, AAMW, SSL, and PKI

e. Delete local certificates and CA profiles

f. Configure and load certificates using an HTTPS connection from AWS

g. Connect to the cloud to retrieve certificates

h. Check license details

i. Add configuration for SSL crypto hardware

j. Download CA and device certificates

k. Load SecIntel and AAMW-cloud certificates

l. Restore previously removed configurations (SecIntel, AAMW, SSL, and PKI)

m. Commit the changes and verify the configuration (SSL Profile, TPM, AAMW profile)

Once all configurations are verified, the SRX Series Firewall establishes a connection with the cloud. A message indicates that the device has been successfully enrolled.

- Script for non-TPM-based devices:

```
request services advanced-anti-malware enroll https://amer.sky.junipersecurity.net/v2/
skyatp/ui_api/bootstrap/enroll/mt8zlb8xwl0vmg5x/8tajwglnz54sdhkn.slax
Platform is supported by ATP Cloud: VSRX.
Version 25.4I-20251117.0.1931 is valid for bootstrapping.
Junos version 25.4I-20251117.0.1931 supports https endpoints.
Enrolling with ATP Cloud license serial number: 060620220302-n41jy.
Going to enroll single device for VSRX: 106616265e0d@060620220302-n41jy with hostname
argon-vsrx-01.
Application Signature DB version on this device is: 3814 (Major). Using latest version of
Application Signature DB is recommended.
Remove related security-intelligence service configurations...
Remove related advanced-anti-malware service configurations...
Remove related SSL service configurations...
Remove related PKI configurations...
Clear local certificate aamw-srx-cert...
Clear key pair: aamw-srx-cert...
Clear CA profile aamw-cloud-ca...
Clear CA profile aamw-secintel-ca...
Building aws certificates...
Configure aws CA...
Load aws CA...
Communicate with cloud...
License type for this device: premium.
License of your device will expire in 215 days.
Configure CA aamw-ca...
Request aamw-secintel-ca CA...
Wait aamw-secintel-ca CA download status...
Load aamw-secintel-ca CA...
Request aamw-cloud-ca CA...
```

```
Wait aamw-cloud-ca CA download status...
Load aamw-cloud-ca CA...
Retrieve CA profile aamw-ca...
CA certificate ready: aamw-ca...
CA certificate ready: aamw-cloud-ca...
CA certificate ready: aamw-secintel-ca...
Generate key pair: aamw-srx-cert...
Enroll local certificate aamw-srx-cert with CA server...
Configure SSL service...
Configuration added successfully for SSL service.
Configure advanced-anti-malware service...
Configuration added successfully for advanced-anti-malware service.
Configure security-intelligence service...
Configuration added successfully for security-intelligence service.
Check configuration on device...
SSL profile:                          [OK]
SecIntel CA:                          [OK]
Cloud CA:                             [OK]
Client cert found:                    [OK]
SSL profile action:                   [OK]
URL for advanced-anti-malware:        [OK]
Profile for advanced-anti-malware:    [OK]
URL for security-intelligence:        [OK]
Profile for security-intelligence:    [OK]
All configurations are correct for enrollment.
Communicate with cloud...
Wait for aamw connection status...
Device enrolled successfully!
Please see following links for more information:
ATP Cloud sample config:
https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/example/
configuration/sky-atp-policy-creating-cli.html
ATP Cloud quick start guide:
http://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-
products/topic-collections/sky-atp-qsg.pdf
ATP Cloud technical documents:
http://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-
products/pathway-pages/index.html
It is recommended to run diagnostic process with the following cli command to make sure
all configurations are valid:
request services advanced-anti-malware diagnostics srxapi.preprod.sky.junipersecurity.net
detail
```

This script performs the following series of checks and configurations to ensure connectivity with Juniper ATP Cloud:

a. Detect if the SRX Series Firewall is a TPM-supported platform

b. Verify whether the Junos OS version supports HTTPS endpoints

c. Identify the device type (standalone or chassis cluster)

d. Remove any existing configuration related to Juniper ATP Cloud enrollment on SecIntel, AAMW, SSL, and PKI

e. Delete local certificates and CA profiles

f. Configure and load certificates using an HTTPS connection from AWS

g. Connect to the cloud to retrieve certificates

h. Check license details

i. Download CA and device certificates

j. Load SecIntel and AAMW-cloud certificates

k. Restore previously removed configurations (SecIntel, AAMW, SSL, and PKI)

l. Commit the changes and verify the configuration (SSL Profile, TPM, AAMW profile)

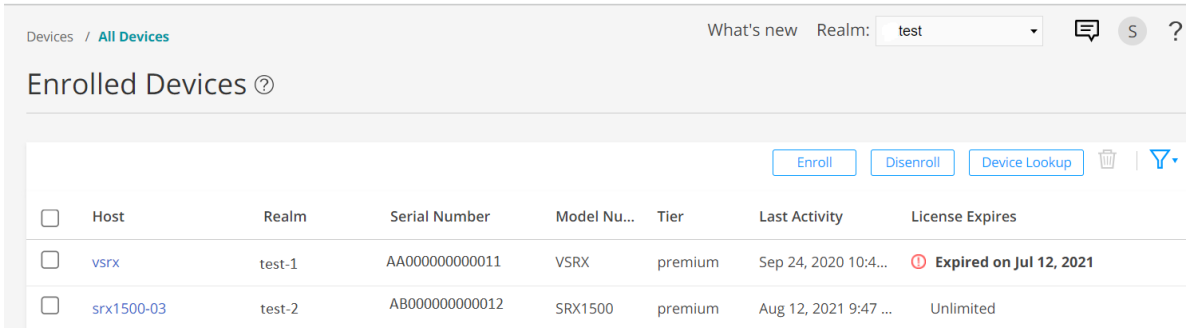
Once all configurations are verified, the SRX Series Firewall establishes a connection with the cloud. A message indicates that the device has been successfully enrolled.

NOTE: If for some reason the ops script fails, disenroll the device (see "Remove an SRX Series Firewall from Juniper ATP Cloud" on page 58) and then re-enroll it.

4. In the Juniper ATP Cloud Web portal, click **Devices**.

   The SRX Series Firewall you enrolled now appears in the table. See Figure 12 on page 34.

Figure 12: Example Enrolled SRX Series Firewall



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

```
show services advanced-anti-malware status
Server connection status:
  Server hostname:  https://amer.sky.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 Firewall communicates to the cloud through multiple persistent connections that are established over a secure channel (TLS 1.2). The SRX Series Firewall is authenticated using SSL client certificates.

As stated earlier, the script performs basic Juniper ATP Cloud configuration on the SRX Series Firewall. These configurations include:

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

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

Table 4: Customer Portal URLs

Location	Customer Portal URL
United States	Customer Portal: **https://amer.sky.junipersecurity.net**
European Union	Customer Portal: **https://euapac.sky.junipersecurity.net**
APAC	Customer Portal: **https://apac.sky.junipersecurity.net**
Canada	Customer Portal: **https://canada.sky.junipersecurity.net**

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

- Configuring the SSL proxy.

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

- Configuring the cloud feeds (allowlists, blocklists and so on.)

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

Juniper ATP Cloud 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.

```
request security pki local-certificate load filename ssl_proxy_ca.crt key sslserver.key
certificate-id ssl-inspect-ca
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 keypair.
ssl-inspect-ca	Is the certificate ID that SSL forward proxy uses in configuring the root-ca in the SSL forward proxy profile.
certificate-chain	Is the file containing the chain of certificates.

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

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

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

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

2

PART

Juniper ATP Cloud Web Portal

CHAPTER 3

Juniper ATP Cloud Web Portal Overview

IN THIS CHAPTER

Juniper ATP Cloud Web UI Overview

IN THIS SECTION

The Juniper ATP Cloud Web UI is a web-based service portal that allows you to monitor Juniper ATP Cloud features enabled through your SRX Series Firewalls. The Juniper ATP Cloud based services are hosted in the Juniper cloud and are maintained and managed by Juniper Networks.

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

You can perform the following tasks with the Web UI:

- Monitoring—Display following information:

  - Verdict of scanned files (clean or malware)
  - Blocked access to known Command and Control (C&C) sites
  - Infected hosts, including their current and past threats
  - Details of exfiltration attempts
  - Discovered Internet of Things (IoT) devices
  - Quarantined emails with malware
  - Other attacks related to the Domain Name System (DNS) and Secure Sockets Layer (SSL).
- Configuring—Configure following features:
  - Create and view allowlists and blocklists that list safe or harmful network nodes
  - Create and view access to different categories of feeds
  - Share threat intelligence captured through malware analysis
  - Configure email quarantine settings and profiles that determine which file types to submit to Juniper ATP Cloud 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.

Accessing the Web UI

To access the Juniper ATP Cloud Web UI:

1. Open a browser that has HTTP or HTTP over SSL (HTTPS) enabled.

   For information on supported browsers and their version numbers, see Juniper ATP Cloud Web UI Browser Support Table.

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

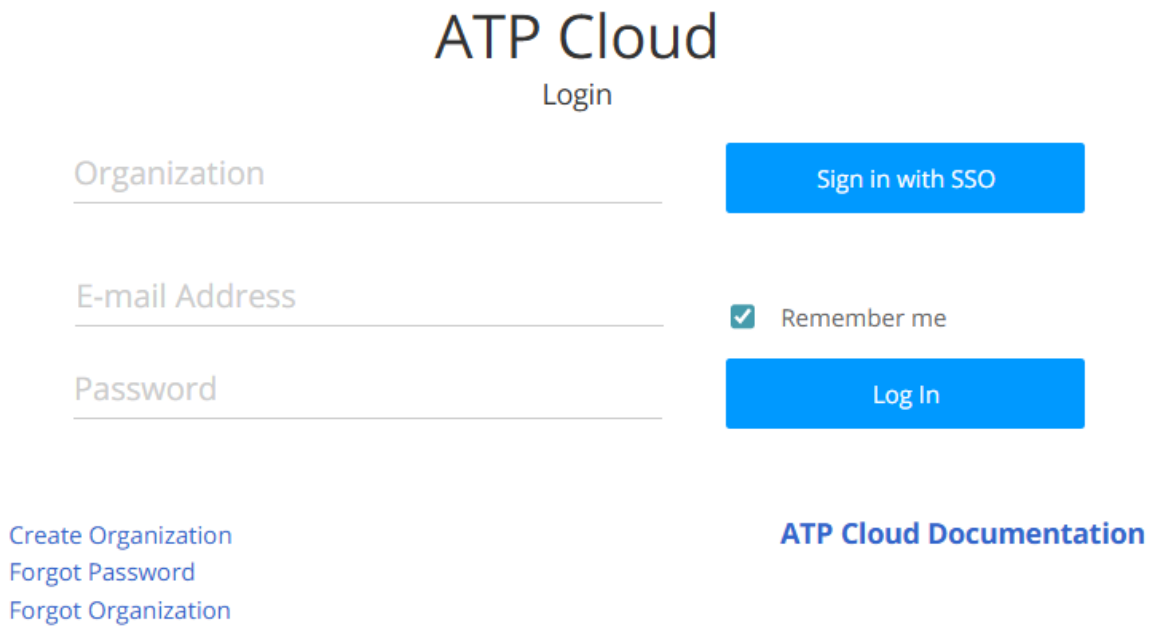
   The customer portal hostname varies by location. See Table 5 on page 40 for customer portal URLs by location.

Table 5: Customer Portal URLs

Location	Customer Portal URL
United States	Customer Portal: **https://amer.sky.junipersecurity.net**
European Union	Customer Portal: **https://euapac.sky.junipersecurity.net**
APAC	Customer Portal: **https://apac.sky.junipersecurity.net**
Canada	Customer Portal: **https://canada.sky.junipersecurity.net**

The Web UI login page appears. See Figure 13 on page 40.

Figure 13: Juniper ATP Cloud Web UI Login Page



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

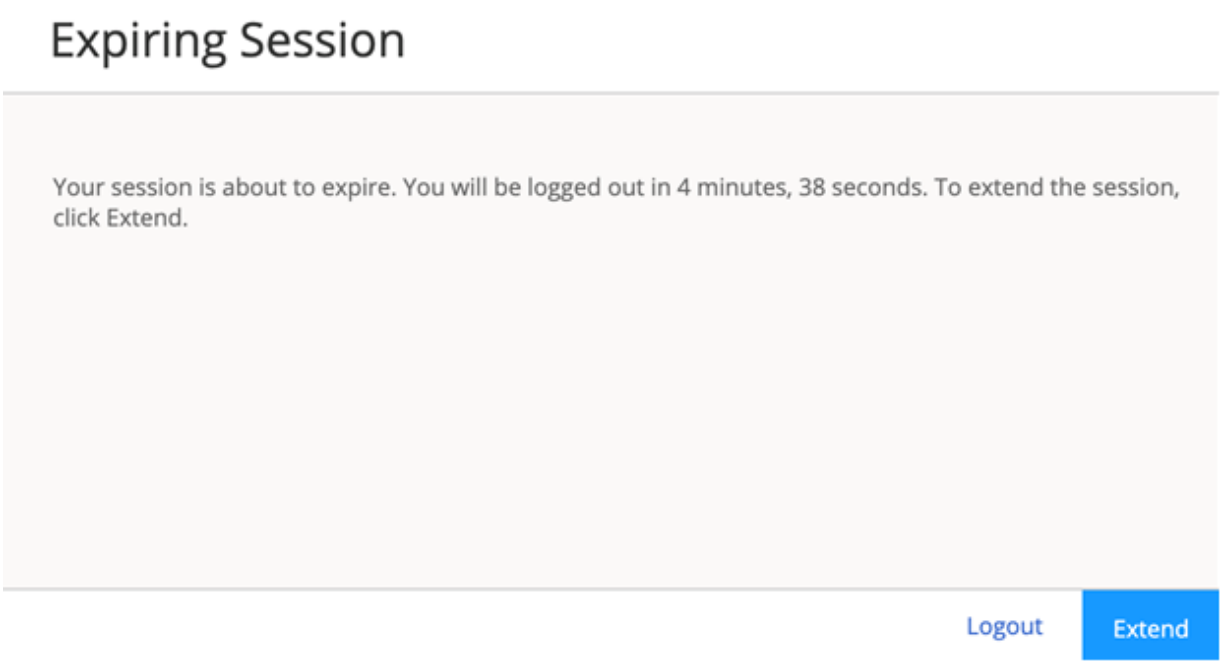
   The Web UI Dashboard page appears.

NOTE: Users can login to Juniper ATP Cloud using different organizations. You can manage organizations using the **Configure** > **Misc Configuration** > **Organization Management** page. See "Organization Overview" on page 224. You must be a system administrator to see the Organization Management page. See "Create and Edit User Profiles" on page 241 for information on role-based access control.

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

Each ATP Cloud session lasts for 60 minutes. Before a session is about to expire you will receive a notification message as shown in Figure 14 on page 41. To extend the current session, click **Extend**. To logout of the session, click **Logout**. You can extend the session for maximum 25 times, after which the session will logout automatically.

Figure 14: Session Expiry Notification



Juniper ATP Cloud Configuration Overview

Table 6 on page 42 lists the basic steps to configure Juniper ATP Cloud.

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

Table 6: Configuring Juniper ATP Cloud

Task	Description	For Information, See
(optional) Update the administrator profile	Update your administrator profile to add more users with administrator privileges to your organization 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.	"Modify My Profile" on page 239 "Create and Edit User Profiles" on page 241
Enroll your SRX Series Firewalls	Select the SRX Series Firewalls to communicate with Juniper ATP Cloud. 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 Firewall.	"Enroll an SRX Series Firewall Using Juniper ATP Cloud Web Portal" on page 51
Set misc configurations	Select **Configure > Misc 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
(optional) Create allowlists and blocklists	Create allowlists and blocklists to list network nodes that you trust and don't trust. Allowlisted websites are trusted websites where files downloaded from do not need to be inspected. Blocklisted websites are locations from which downloads should be blocked. Files downloaded from websites that are not in the allowlist or blocklist are sent to the cloud for inspection. This step is done in the Web UI.	"Create Allowlists and Blocklists" on page 168

Table 6: Configuring Juniper ATP Cloud *(Continued)*

Task	Description	For Information, See
(optional) Create the Juniper ATP Cloud profile	Juniper ATP Cloud profiles define which file types are to be sent to the cloud for inspection. For example, you might want to inspect executable files but not documents. If you don't create a profile, the default one is used. This step is done in the Web UI.	"File Inspection Profiles Overview" on page 190
(optional) Identify compromised hosts	Compromised hosts are systems where there is a high confidence that attackers have gained unauthorized access. Once identified, Juniper ATP Cloud recommends an action and you can create security policies to take enforcement actions on the inbound and outbound traffic on these infected hosts. This step is done on the SRX Series Firewall.	"Compromised Hosts: More Information" on page 81
(optional) Block outbound requests to a C&C host	The SRX Series Firewall 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. This step is done on the SRX Series Firewall. **NOTE**: Requires Juniper ATP Cloud license. For more information, see Software Licenses for ATP Cloud.	"Command And Control Servers: More Information" on page 95
Configure the Advanced Anti-Malware Policy on the SRX Series Firewall	Advanced anti-malware security policies reside on the SRX Series Firewall 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. This step is done on the SRX Series Firewall.	Juniper Advanced Threat Prevention Cloud Policy Overview
Configure the SecIntel Policy on the SRX Series Firewall	Create the SecIntel policies on the SRX Series Firewall to act on infected hosts and attempts to connect with a C&C server. This step is done on the SRX Series Firewall.	Configure the SRX Series Firewall to Block Infected Hosts Configure the SRX Series Firewall to Block Outbound Requests to a C&C Host

Table 6: Configuring Juniper ATP Cloud *(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 Firewall.	Configure the SRX Series Firewall to Block Infected Hosts Configure the SRX Series Firewall to Block Outbound Requests to a C&C Host Example: Configure Juniper Advanced Threat Prevention Cloud Policy

You can optionally use APIs for C&C feeds, allowlist and blocklist operations, and file submission. See the Threat Intelligence Open API Setup Guide for more information.

NOTE: The cloud sends data, such as your Juniper ATP Cloud allowlists, blocklists and profiles, to the SRX Series Firewall every few seconds. You do not need to manually push your data from the cloud to your SRX Series Firewall. Only new and updated information is sent; the cloud does not continually send all data.

Dashboard Overview

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

The Web UI for Juniper ATP Cloud 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.

NOTE: The data on the Web UI dashboard is updated on hourly checks; it does not get updated in real-time.

In addition, you can use the dashboard to:

- Navigate to the Files 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 Threat Source widget.

Available dashboard widgets are as follows:

Table 7: Juniper ATP Cloud 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 | 46

About Juniper ATP Cloud | 2

How Is Malware Analyzed and Detected? | 10

Hosts Overview | 75

HTTP File Download Overview | 104

Command And Control Servers: More Information | 95

Reset Password

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

- To reset your password you must enter the organization 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 "Modify My Profile" on page 239 for those instructions.

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

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

Modify My Profile | 239

Create and Edit User Profiles | 241

Dashboard Overview | 44

Recover Organization Name

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

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

```
Welcome to Juniper ATP Cloud!

You have successfully created your ATP Cloud Organization. Below is your information:
You email ID: user@juniper.net
 Organization Name: " organization123"

You may save the Organization name for future use for login purpose as ATP Cloud login
expects Organization name as an input.

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

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

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

- Click **Forgot Organization** link from the Juniper ATP Cloud login page.

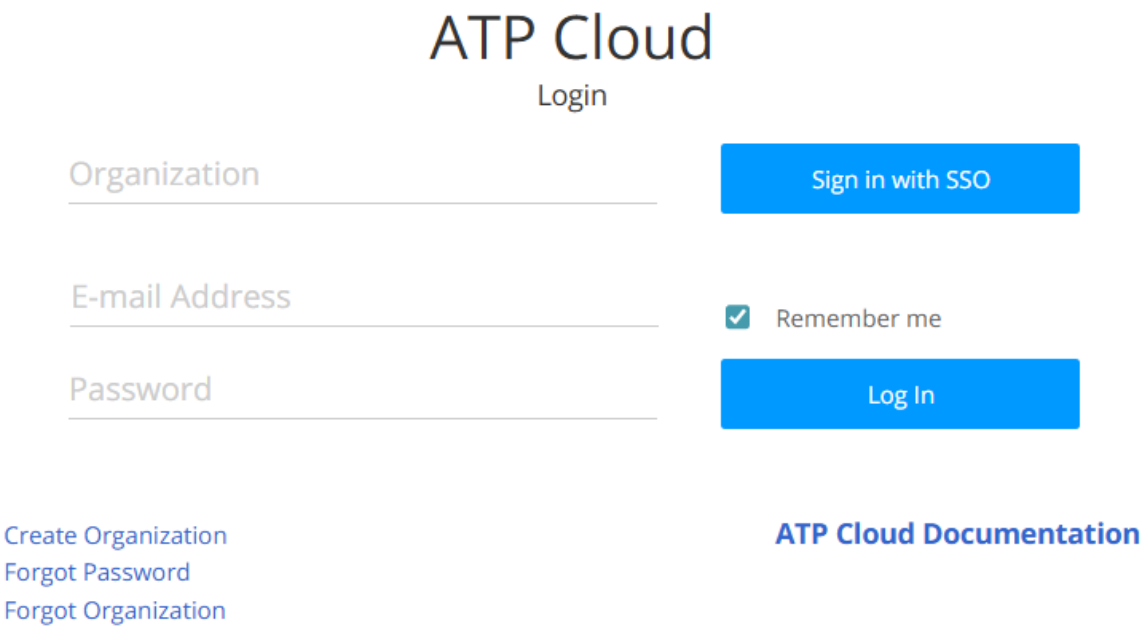
The following section provides details to recover the organization name using the Juniper ATP Cloud web portal.

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

To recover the organization name from the ATP Cloud web portal:

1. Open a Web browser, type in the URL for the ATP Cloud web portal, and press **Enter**.
   The login page appears as shown in Figure 15 on page 48.

Figure 15: Juniper ATP Cloud Web UI Login Page



2. Click the **Forgot Organization** link.

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

3. Click **Continue**.

   The customer support center login page appears.

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

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

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

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

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

     ```
     Welcome to Juniper ATP Cloud !

     Based on your request please find below Organizations created by you with Juniper ATP
     Cloud till date.
     ```

```
Your email ID : <Juniper-Networks-Account>

 Organization names: Organization-1, Organization-2, Organization-3…Organization-N

You may save the Organization name for future use for login purpose as ATP Cloud login
expects Organization name as an input.

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

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

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

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

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

5. Click **OK** to login to the ATP Cloud portal with the organization name.

RELATED DOCUMENTATION

Reset Password | 46

Dashboard Overview | 44

3

PART

Enroll SRX Series Firewalls in Juniper ATP Cloud Web Portal

CHAPTER 4

Enroll and Manage SRX Series Firewalls

IN THIS CHAPTER

Enroll an SRX Series Firewall Using Juniper ATP Cloud Web Portal

IN THIS SECTION

You can enroll SRX Series Firewalls using the Juniper ATP Cloud Web Portal.

Before You Begin

- Check whether the device is already enrolled. For more information, see "Search for SRX Series Firewalls Within Juniper ATP Cloud" on page 59.
- If the IPv6 dual-stack (both IPv4 and IPv6) support is enabled on your SRX Series Firewall, run the following CLI commands:

  1. `set services advanced-anti-malware connection protocol-family inet6`—Configure the IPv6 protocol for AAMW connection.
  2. (Optional) `set services advanced-anti-malware connection proxy-profile` *`proxy-profile-name`*—Configure a proxy profile name if you have configured a proxy server and your Internet access goes through it.

3. (Optional) `set services advanced-anti-malware connection routing-instance` *routing-instance-name*— Configure a routing instance name if you plan to route using a specific routing instance.

- Ensure that traffic is allowed to the junipersecurity.net domain on ports 443, 8443, and 8080.

To enroll a device in Juniper ATP Cloud using the Web Portal:

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 Firewall you want to enroll with Juniper ATP Cloud and press `Enter`. (Note that this command must be run in operational mode.)

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

(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 Firewall.

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

In the Enrolled Devices page, basic connection information for all enrolled devices is provided. This information includes serial number, model number, tier level enrollment status in Juniper ATP Cloud, 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

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

Table 8: Button Actions *(Continued)*

Actions	Definition
NOTE: • When you run the Enroll or Disenroll command, the SRX Series Firewall commits any uncommitted configuration changes. • Generating a new Enroll command or Disenroll command invalidates any previously generated commands.	
Device Lookup	Use the **Device Lookup** button to search for the device serial number(s) in the licensing database to determine the tier of the device. For this search, the device does not have to be currently enrolled in Juniper ATP Cloud.
Remove	Removing an SRX Series Firewall is different than disenrolling it. Use the Remove option only when the associated SRX Series Firewall is not responding (for example, hardware failure). Removing it, disassociates it from the cloud without running the Junos OS 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 primary. The cloud will detect that this is a cluster and will automatically enroll both the primary and backup as a pair. Both devices, however, must be licensed accordingly.

NOTE: Juniper ATP Cloud supports both active/active and active/passive cluster configurations. The passive (non-active) node does not establish a connection to the cloud until it becomes the active node.

NOTE: The License Expiration column contains the status of your current license, including expiration information. There is a 60 day grace period after the license expires before the SRX Series Firewall is disenrolled from Juniper ATP Cloud.

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

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

In the Enrolled Devices page, you can view the organization with which the device is associated. From the Organization Management page, you can change that organization association or attach new organizations. See "Organization Management" on page 226 for configuration details.

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

Juniper ATP Cloud uses a Junos OS op script to help you configure your SRX Series Firewall to connect to the Juniper ATP Cloud service. This script performs the following tasks:

- Downloads and installs certificate authority (CA) licenses onto your SRX Series Firewall.

  NOTE:

  - You must allow traffic to the junipersecurity.net domain on ports 8444 and 7444 since the Trusted Platform Module (TPM)-based certificates are used for connections between the SRX Series Firewall and Juniper ATP Cloud. To determine if a feature is supported by a specific platform or Junos OS release, see Feature Explorer. For more information about using TPM on SRX Series Firewalls, see Trusted Platform Module Overview.
  - For newly enrolled TPM and non-TPM-based devices, traffic must be allowed to the junipersecurity.net domain only on port 443.

- Creates local certificates and enrolls these certificates with the cloud server.
- Performs basic Juniper ATP Cloud configuration on the SRX Series Firewall.
- Establishes a secure connection to the cloud server.

NOTE:

- Juniper ATP Cloud requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) can connect to the Internet.
- The data plane connection should not be sourced from the management or loopback interface, such as fxp0 or lo0. You do not need to open any ports on the SRX Series Firewall to communicate with the cloud server. However, if you have a device in the middle, such as a firewall, then that device must have port 443 open.

- The SRX Series Firewall uses the default inet.0 routing table and an interface part of inet.0 as source-interface for control-plane connection from SRX Series Firewall to Juniper ATP Cloud. If the only Internet-facing interface on SRX Series Firewall is part of a routing instance, then we recommend that you add a static route pointing to the routing instance. Else, the control connection will fail to establish.
- Juniper ATP Cloud requires that your SRX Series Firewall hostname contains only alphanumeric ASCII characters (a-z, A-Z, 0-9), the underscore symbol (_) and the dash symbol (-).

WARNING: If you are configuring explicit web proxy support for SRX Series Firewall/ Juniper ATP Cloud connections, you must enroll SRX Series Firewalls to Juniper ATP Cloud using a slightly different process. See Explicit Web Proxy for Juniper ATP Cloud.

Enroll devices using Juniper Security Director Cloud Portal

You can enroll SRX Series Firewalls in the Juniper ATP Cloud using the Juniper Security Director Cloud Portal. In the Enrolled Devices page, the devices enrolled through the Juniper Security Director Cloud Portal display (SDC) next to their hostnames.. For more information, see Juniper Security Director Cloud User Guide.

RELATED DOCUMENTATION

Juniper ATP Cloud RMA Process | 62

Remove an SRX Series Firewall from Juniper ATP Cloud | 58

Search for SRX Series Firewalls Within Juniper ATP Cloud | 59

Device Information | 62

Enroll an SRX Series Firewall in Juniper ATP Cloud Using J-Web

You can also enroll an SRX Series Firewall to Juniper ATP Cloud using J-Web. J-Web is the Web interface that comes preinstalled on the SRX Series Firewall. For more information, see J-Web User Guide for SRX Series Firewalls.

Before You Begin

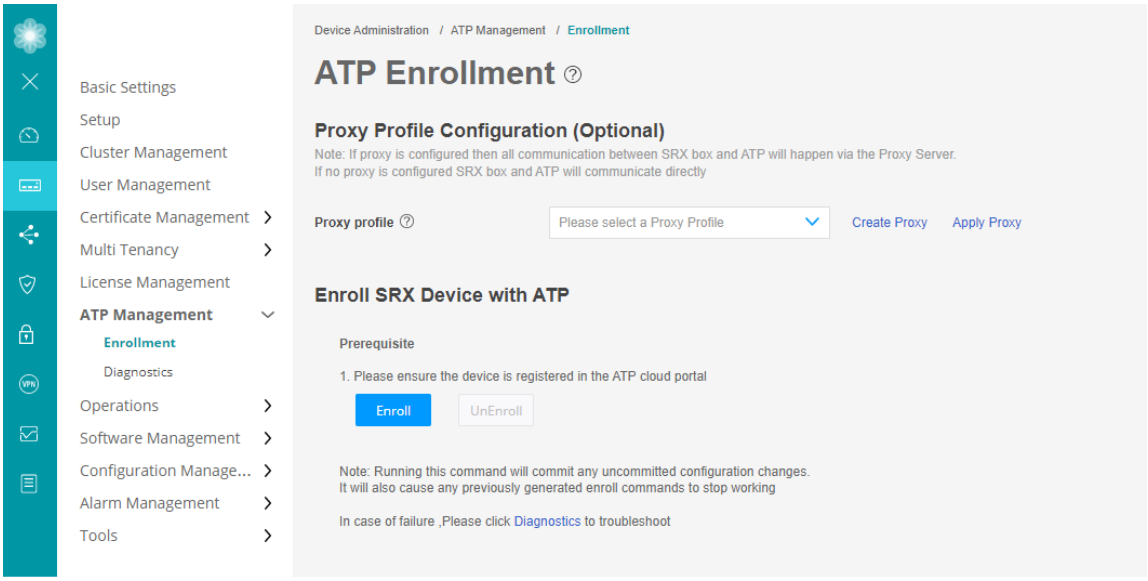
- Decide which region the realm you create will cover because you must select a region when you configure a realm.

- Check whether the device is already enrolled in the Juniper ATP Cloud Web Portal.
- In CLI mode, configure `set security forwarding-process enhanced-services-mode` on your SRX300, SRX320, SRX340, SRX345, and SRX550M devices to open ports and get the device ready to communicate with Juniper ATP Cloud

To enroll your SRX Series Firewall using J-Web portal:

1. Log in to J-Web. For more information, see Start J-Web.
2. (Optional) Configure a proxy profile.
   a. In the J-Web UI, navigate to **Device Administration** > **ATP Management** > **Enrollment**.

      The ATP Enrollment page is displayed.



   b. Use either of the following methods to configure the proxy profile:

      - Select an existing proxy profile from the Proxy Profile list.

        NOTE:

        - The list displays the existing proxy profiles created using the Proxy Profile page (**Security Policies & Objects** > **Proxy Profiles**).
        - The SRX Series Firewall and Juniper ATP Cloud communicate through the proxy server if a proxy profile is configured. Otherwise, they directly communicate with each other.

      - Click **Create Proxy** to create a proxy profile.

The Create Proxy Profile page appears.

Complete the configuration:

- **Profile Name**—Enter a name for the proxy profile.
- **Connection Type**—Select the connection type server (from the list) that the proxy profile uses:
  - **Server IP**—Enter the IP address of the proxy server.
  - **Host Name**—Enter the name of the proxy server.
- **Port Number**—Select a port number for the proxy profile. Range is 0 through 65,535.

Click **OK**.

A new proxy profile is created.

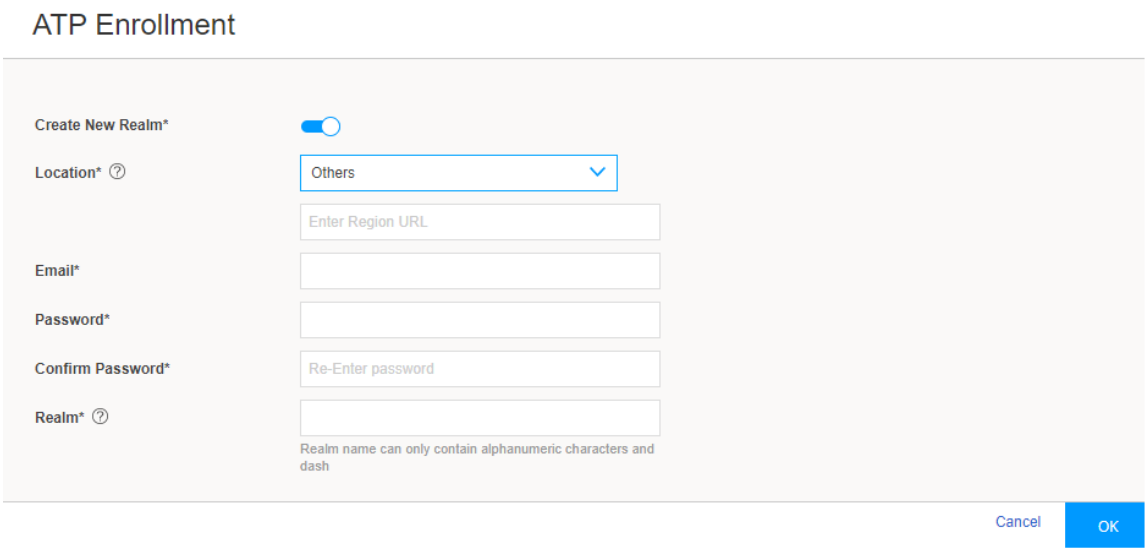
c. Click **Apply Proxy**.

Applying proxy enables the SRX Series Firewall and Juniper ATP Cloud to communicate through the proxy server.

3. Enroll your device to Juniper ATP Cloud.

a. Click **Enroll** to open the ATP Enrollment page.

NOTE: If there are any existing configuration changes, a message appears for you to commit the changes and then to proceed with the enrollment process.



b. Complete the configuration:

- **Create New Realm**—By default, this option is disabled if you have a Juniper ATP Cloud account with an associated license. Enable this option to add a new realm if you do not have a Juniper ATP Cloud account with an associated license.
- **Location**—By default, the region is set as **Others**. Enter the region URL.
- **Email**—Enter your e-mail address.
- **Password**—Enter a unique string at least eight characters long. Include both uppercase and lowercase letters, at least one number, and at least one special character. Avoid using spaces, and you cannot use the same sequence of characters that are in your e-mail address.
- **Confirm Password**—Reenter the password.
- **Realm**—Enter a name for the security realm. This name should be meaningful to your organization. A realm name can contain only alphanumeric characters and the dash symbol. Once created, this name cannot be changed.

c. Click **OK**.

The status of the SRX Series Firewall enrollment process is displayed.

NOTE: Click **Diagnostics** to troubleshoot any enrollment errors.

Remove an SRX Series Firewall from Juniper ATP Cloud

If you no longer want an SRX Series Firewall to send files to the cloud for inspection, use the disenroll option to disassociate it from Juniper ATP Cloud. The disenroll process generates an ops script to be run on SRX Series Firewalls and resets any properties set by the enroll process.

To disenroll an SRX Series Firewall:

1. Select the check box associated with the device 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

Search for SRX Series Firewalls Within Juniper ATP Cloud | 59

Search for SRX Series Firewalls Within Juniper ATP Cloud

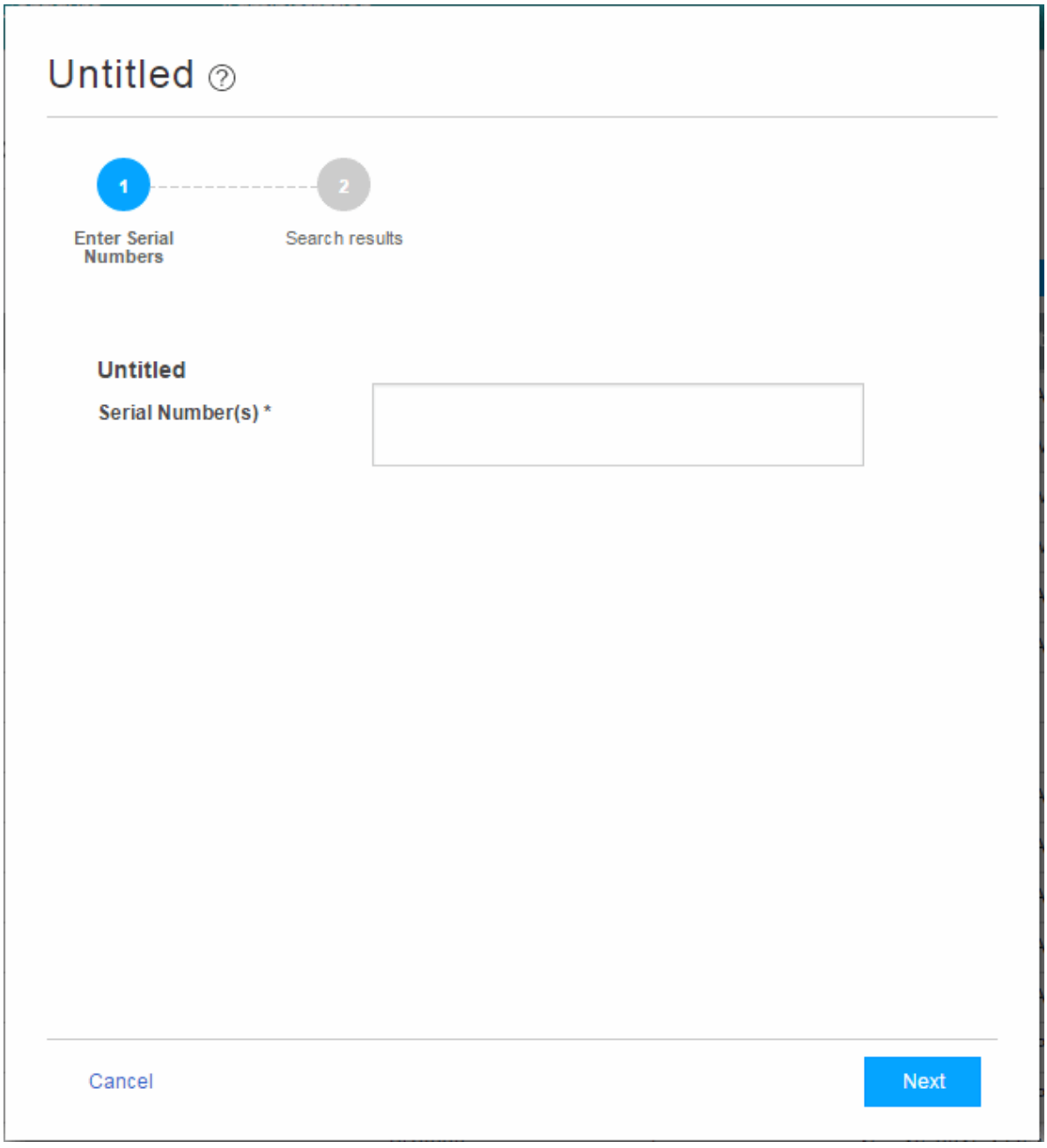
You can search for any SRX Series Firewall enrolled within your organization of Juniper ATP Cloud using the **Device Lookup**option. This option also allows you to see the type of license the device is utilizing. You can only search for device using the serial numbers.

To search for devices enrolled with Juniper ATP Cloud:

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

   The Device Lookup window appears. See Figure 16 on page 60.

Figure 16: Searching for a Device in the Web UI

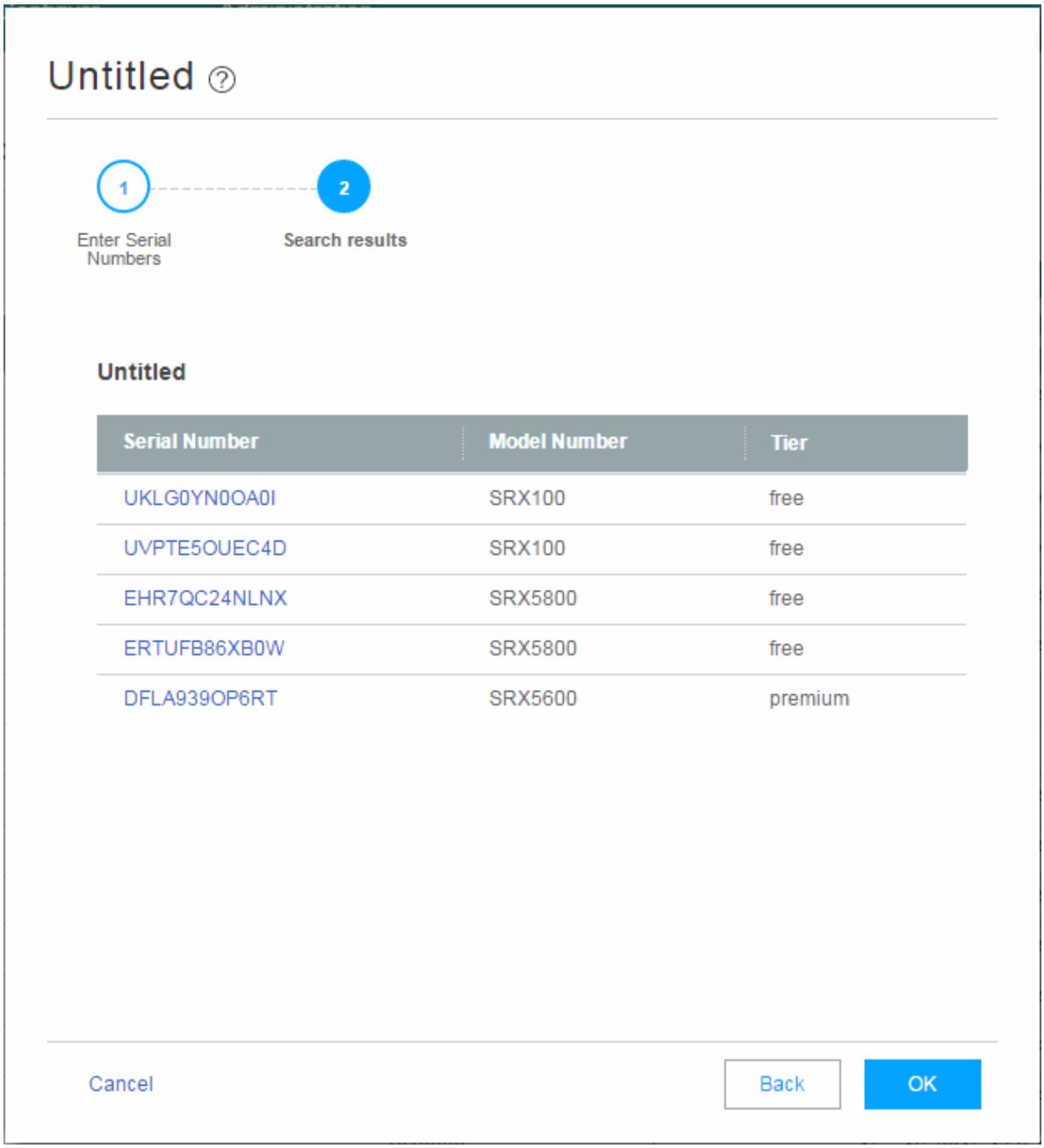


3. Enter the serial number of the device you want to search for and click **Next**. You can enter multiple serial numbers, separating each entry with a comma. For more information, see the infotips.

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 61.

Figure 17: Example Device Search Results



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

RELATED DOCUMENTATION

Device Information | 62

Enroll an SRX Series Firewall Using Juniper ATP Cloud Web Portal | 51

Remove an SRX Series Firewall from Juniper ATP Cloud | 58

Juniper ATP Cloud RMA Process

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

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

WARNING: After any serial number change on the SRX Series Firewall, a new RMA serial number needs to be re-enrolled with Juniper ATP Cloud cloud. This means that you must enroll your replacement unit as a new device. See Enroll an SRX Series Firewall using Juniper ATP Cloud Web Portal. Juniper ATP Cloud 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 Firewall from the old device.

Device Information

Use this page to view the following information about the selected SRX Series Firewall.

Table 9: Device Information Fields

Field	Definition
Device Information	
Serial Number	SRX Series Firewall serial number

Table 9: Device Information Fields *(Continued)*

Field	Definition
Host	Hostname of the device Devices enrolled through the Juniper Security Director Cloud Portal display (SDC) next to their hostnames.
Model Number	SRX Series Firewall model number
Tier	License type
OS Version	SRX Series Firewall Junos OS version
Submission Status	Allowed or Paused This status indicates whether the device can submit files to Juniper ATP Cloud or if it has reached its daily limit. See "File Scanning Limits" on page 123.
Configuration Information	
Global Config	The Device and Cloud fields indicate the version numbers of each list, both on the device and in the cloud. You can compare them to see if they are in sync.
Profile Config	
Global Allowlist	
Global Blocklist	
Global DNS Allowlist	
Global DNS Blocklist	
Customer Allowlist	

Table 9: Device Information Fields *(Continued)*

Field	Definition
Customer Blocklist	
Customer ETA Allowlist	
PHASE Signature	
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 C&C event was received.

RELATED DOCUMENTATION

- Enroll an SRX Series Firewall Using Juniper ATP Cloud Web Portal | **51**
- Remove an SRX Series Firewall from Juniper ATP Cloud | **58**
- Search for SRX Series Firewalls Within Juniper ATP Cloud | **59**

4

PART

Monitor Juniper ATP Cloud Features

CHAPTER 5

Reports

IN THIS CHAPTER

Reports Overview

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

The generated report will contain categories such as the following:

Table 10: PDF Report Contents

Report Category	Definition

Executive Summary	An overview report data separated into following categories:
	• Malware—Lists newly discovered malware and known malware.
	• C&C Server Destinations—Lists C&C server destination.
	NOTE: The criterion to display the C&C server destination in the reports is that the threat level must be equal to or greater than 7.
	• Hosts with Malicious Activities—Lists the following:
	  • Infected hosts—Lists the number of potentially infected hosts whose threat level is less than the threshold threat level that is set by the customer.
	  • Blocked hosts—Lists the number of infected hosts that have met the threshold threat level and is blocked by policies configured on the SRX Series Firewall.
	• Domains and URLs—Lists the suspicious or risky domains and URLs
	• High-risk User Data—Lists the following:
	  • Users' computers infected with malware.
	  • High-risk websites accessed by users.
	• DNS DGA—Lists the DNS-DGA query counts for the top host IP addresses.
	• DNS Tunnels—Lists the DNS tunnel counts for the top host IP addresses.
	• ETI Source Hosts—Lists the ETI detection counts for the top host IP addresses.
	• ETI Destinations—Lists the ETI detection counts for the top Server Name Indication (SNI) domains.

Table 10: PDF Report Contents *(Continued)*

Report Category	Definition
Malware	The malware section contains the following information: • Top Malware Identified—Lists the names of the top malware by count. • Top Infected File MIME Types—Lists the top infected multi-purpose Internet mail extensions (MIME) by count. • Top Scanned File Categories—Lists the top file categories that are scanned.
C&C Server and Malware Locations	This section contains the following information: • Top C&C Server Location by Count—Lists the top countries for command and control (C&C) servers by number of communication attempts (C&C hits). • Top Malware Threat Locations by Count—Lists the top countries with malware threats.
ETI Server Locations	This section contains the following information: • Top ETI Server Locations by Count—Lists the top countries for ETI servers by number of communication attempts (ETI hits).

Table 10: PDF Report Contents *(Continued)*

Report Category	Definition

DNS	This section contains the following information:
	• DNS Event Counts—Lists the following:
	  • DNS-DGA Events—Lists the number of DGA events seen by ATP Cloud for the customer over the time period that the report covers.
	  • DNS Tunnel Events—Lists the number of Tunnel events seen by ATP Cloud for the customer over the time period that the report covers.
	• Top DNS Tunnel Destination Domains—Lists the top tunnel domains seen by ATP Cloud and number of events involving those domains for the customer over the time period that the report covers.

Hosts	This section contains the following information: • Top Compromised Hosts—Lists the top hosts that might have been compromised based on their associated threat level.
Risky Files	This section contains the following information: • Top Risky File Categories by Count—Lists the top risky file categories by count for known and newly discovered malicious files. • Top Risky Files Detected by Count—Lists the top risky files detected by count. • Top IPs Detected Attempting to Access Risky Files by Count—Lists the top IP addresses attempting to access risky files. • Top Risky Files Detected per Top Users—Lists the top risky files detected per top users attempting to access the files.

Table 10: PDF Report Contents *(Continued)*

Report Category	Definition
Risky Domains, URLS, AND IPs	This section contains the following information: top risky domains, URLs, and IP addresses detected by the number of times access was attempted. It also includes the top users who have attempted to access these risky domains, URLs, and IP addresses. • Top Detected Risky Domains, URLs, and IPs by Count—Lists the top risky domains, URLs, and IP addressess detected by the number of times access was attempted. • Most Active Users for Risky Domains, URLs, and IPs by Count—Lists the top users who are most active in attempting to access the risky domains, URLs, and IP addresses by count. • Top Detected Risky Domains, URLs, and IPs by Threat Level —Lists the top risky domains, URLs, and IP addressess detected by the threat level.

Table 10: PDF Report Contents *(Continued)*

Report Category	Definition
Email	This section contains the list of actions taken on scanned emails. It also includes email attachments determined to be malware and users who are risky email senders. • Actions Taken—Lists the action taken for scanned e-mail. • High-Risk Email Data—Lists the count of e-mail attachments with malware and risky senders. • Malicious SMTP Email by Count—The report breaks scanned e-mail down by protocol and lists SMTP e-mails found to be malicious. • Malicious IMAP Email by Count—The report breaks scanned e-mail down by protocol and lists IMAP e-mails found to be malicious. • Top Risky File Categories Detected for Email Attachments—Lists the top risky file categories that were detected from files received as e-mail attachments. • Top Risky Email Attachments Detected by Count—Lists the top risky files that are detected from email attachments. • Top Users Receiving Risky Email Attachments—Lists the top users who are receiving risky file attachments through e-mail. • Top Risky Email Attachments Detected per Top Users—Lists the top users and their most risky file attachments. • Top Risky Email Sender Domains by Count—Lists the top risky sender domains based on the threat level of file attachments sent in email. • Top Sender Domains of Risky File Attachments by Count—Lists the top sender domains with risky file attachments and the count of how many times the the risky file attachments that were detected. • Actions on SMTP Malicious Email by Count—Lists actions taken for malicious SMTP e-mails.

Table 10: PDF Report Contents *(Continued)*

Report Category	Definition
	• Actions on IMAP Malicious Email by Count—Lists actions taken for malicious IMAP e-mails.
Devices	This section contains the following information: • Zero Submissions—Lists the devices that have not submitted files in the past 30 days. • Expiring Devices—Lists the devices that are going to expire in next 60 days.

RELATED DOCUMENTATION

Configure Report Definitions | 72

Configure Report Definitions

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

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

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

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

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

Do the following to configure a custom report definition:

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

Table 11: Report Definition Fields

Field	Description
Name	Enter a name for the report. This is a unique string that must begin with an alphanumeric character and can include dashes, spaces, and underscores; 63-character maximum.
Description	Give the report a detailed description that all administrators can recognize.
Date Range Options	Configure a recurring schedule for running a report. The options are: Last Day (daily), Last Week (once weekly), and Last Month (once monthly). Based on your selection, you will configure more a specific time period in the next field.
Generate Report Every	Use the downward arrow in the entry field for adding multiple days. Use the X to remove a day. If you selected Last Day in the previous field, choose multiple days of the week for running a report. For example, every day (add all days manually Sunday through Saturday) or only add Monday, Wednesday, and Friday for an every other day report. If you selected Last Week, choose one day of the week for running a weekly report. If you selected Last Month, choose whether to run a report on the first day of the month or the last day of the month.
Email Recipients	Once a report is generated, you can have it sent to one or more email addresses. The email addresses available for receiving reports come from the **Administrator** > **Users** list. Note that once the report is created, you can always send it to an email address on-demand by selecting the check box for the report in the list view and clicking the Send button at the top of the page. A new window appears, and you can select an email address there. Again, the available addresses come from the **Administrator** > **Users** list.

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

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

RELATED DOCUMENTATION

Reports Overview | 66

CHAPTER 6

Hosts

IN THIS CHAPTER

Hosts Overview

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

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

NOTE: User notification of infected hosts—As of Junos OS 18.1R1, there is support HTTP URL redirection based on infected hosts with the block action. This is configured through the CLI on the SRX Series Firewall using the `set services security-intelligence profile` command. See security-intelligence(services) for details.

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

- Send junk or spam e-mails 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, 10.130.132.133 and threat level 5. Once threats are identified, you can create threat prevention policies to take enforcement actions on the inbound and outbound traffic on these infected hosts. See "Configuration for Infected Hosts" on page 216 for more information.

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

Table 12: Operations for Multiple Infected Hosts

Action	Definition
Export Data	Click the Export button to download compromised host data to a CSV file. You are prompted to narrow the data download to a selected time-frame.
Set Policy Override	Select the check box beside one or multiple hosts and choose one of the following options: • Never include host(s) in infected hosts feed • Always include host(s) in infected hosts feed • Use configured policy (not included in infected hosts feed) **NOTE**: The policy referred here is the policy configured on the SRX Series Firewall. See Example: Configure Juniper Advanced Threat Prevention Cloud Policy.
Set Investigation Status	Select the check box beside one or multiple hosts and choose one of the following options: In progress, Resolved - false positive, Resolved - fixed, and Resolved - ignored.
NOTE: When you select a **Policy Override** option for hosts, other dependent status fields, such as Infected Host Feed, will also change accordingly. In some cases, you might have to refresh the page to see the updated information.	

The following information is available in the Host table.

Table 13: Compromised Host Information

Field	Description
Host Identifier	The Juniper ATP Cloud-assigned name for the host. This name is created by Juniper ATP Cloud using known host information such as IP address, MAC address, username, and hostname. 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 might appear as any of the following formats: `user01@2001:db8:cc:dd:ee:ff`, `user02@10.1.1.1` or `10.1.1.1` **NOTE**: You can edit this name. If you edit the Juniper ATP Cloud-assigned name, Juniper ATP Cloud will recognize the new name and not override it.
Host IP	The IP address of the compromised host.
Threat Level	A number between 0 -10 indicating the severity of the detected threat, with 10 being the highest **NOTE**: Click the three vertical dots at the top of the column to filter the information displayed on the page by threat level.
Infected Host Feed	Displays the current host feed settings: • 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 allowlisted and will be excluded from the infected host feed even if its threat level meets the threshold. • Excluded Manually: The host is allowlisted manually and will be excluded from the infected host feed even if its threat level meets the threshold. Example: If you do not enable **Add to Infected Hosts** setting while creating a new adaptive threat profiling feed, the feed information will not be sent to the infected host feed. • Included Manually: The host is blocklisted and will be included in infected host feed even if its threat level does not meet the threshold.

Table 13: Compromised Host Information *(Continued)*

Field	Description
Last Host Activity	Displays the date and time of the most recent activity of the threat.
C&C Hits	The number of times a command and control (C&C) server communication threat with this host was detected. **NOTE**: Click the three vertical dots at the top of the column to filter the information displayed on the page by C&C hits.
Malware	The number of times a malware threat was downloaded by this host. **NOTE**: Click the three vertical dots at the top of the column to filter the information displayed on the page by malware detections.
Policy	Displays the current policy settings • Use configured policy • Always include host in infected hosts feed • Never include host in infected hosts feed
State of Investigation	Displays either Open, In progress, Resolved-False positive, Resolved-Fixed, Resolved-Ignored
Source	Displays the source of the threat. For example, API, Detection, Adaptive threat profiling feed, and so on.

RELATED DOCUMENTATION

Host Details | **79**

Configuration for Infected Hosts | **216**

HTTP File Download Overview | **104**

HTTP File Download Details | **107**

Manual Scanning Overview | **122**

Host Details

Access this page by clicking the Host Identifier from the **Monitor** >**Hosts** page. Double-click the host to view summary details and malicious files that have been downloaded.

Use the host details page to view in-depth information about current threats to a specific host by time frame.

For C&C threat sources, you can change the host ID, the investigation status, and the blocked status of the host.

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

Table 14: Threat Level Recommendations

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

- Host Identifier—Displays the Juniper ATP Cloud-assigned name of the host. You can edit this name by entering a new name in this field and clicking **Save**. To return to the default assigned name, click **Reset**.
- Host IP Address—Displays the IP address of the selected host.
- MAC Address—This information is only available when Juniper ATP Cloud 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 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 | **75**

HTTP File Download Overview | **104**

HTTP File Download Details | **107**

Manual Scanning Overview | **122**

CHAPTER 7

Identify Infected Hosts

IN THIS CHAPTER

Compromised Hosts: More Information

IN THIS SECTION

Infected hosts are systems where there is 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-mails to attack other systems or distribute illegal software.
- Collect personal information, such as passwords and account numbers.
- Disable your computer's security settings to allow easy access.

Infected hosts are listed as IP address or IP subnet of the host along with a threat level, for example, xxx.xxx.xxx.133 and threat level 5. Once identified, Juniper ATP Cloud recommends an action and you can create security policies to take enforcement actions on the inbound and outbound traffic on these infected hosts. Juniper ATP Cloud 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 Firewall. See "Download And Run the Juniper ATP Cloud Script" on page 26.

Figure 18 on page 82 shows one example of how devices are labelled as infected hosts by downloading malware.

Figure 18: Infected Host from Malware

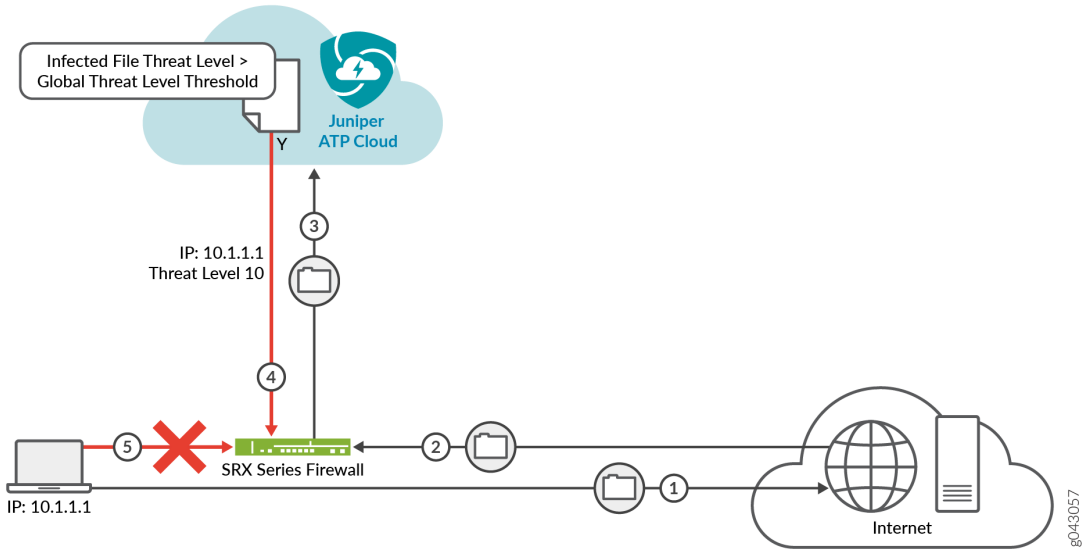


Table 15: Identifying Infected Hosts

Step	Description
1	A client with IP address 10.1.1.1 is located behind an SRX Series Firewall and requests a file to be downloaded from the Internet.
2	The SRX Series Firewall 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 Firewall has a Juniper ATP Cloud 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. The SRX Series Firewall sends the file to the client while the cloud performs an exhaustive inspection.

Table 15: Identifying Infected Hosts *(Continued)*

Step	Description
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 Firewall. The client is placed on the infected host list.
5	Juniper ATP Cloud blocks the client from accessing the Internet. The client remains on the infected host list until an administrator performs further analysis and determines it is safe.

You can view the status of hosts from the Juniper ATP Cloud Web Portal by navigating to **Monitor**>**Hosts**. You can also use the `show services security-intelligence statistics` CLI command on the SRX Series Firewall 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 > Infected Hosts** window to alert users when a host's threat level is at or above a specified threshold.

A malware and host status event syslog message is created in `/var/log/messages`. Junos OS supports forwarding logs using stream mode and event mode.

NOTE: To use syslog, you must configure system logging for all SRX Series Firewall within the same organization. For example, if Organization1 contains SRX1 and SRX2, both SRX1 and SRX2 must have system logging enabled. For more information about 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:

Table 16: Syslog Record Fields

Field	Description
timestamp	Date and time of syslog entry
tenant_id	Internal unique ID
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 Juniper ATP Cloud 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 Firewall silently drops the session's packet and the session eventually times out. If block close is configured, the SRX Series Firewalls 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 about setting block drop and block close, see Configure the SRX Series Firewall to Block Infected Hosts.

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 about the host details, see the web UI tooltips and online help.

You can also use the `show security dynamic-address category-name Infected-Hosts` CLI command to view the infected host list.

```
host> show security dynamic-address category-name Infected-Hosts
No.      IP-start        IP-end          Feed             Address
1        x.0.0.7         x.0.0.7         Infected-Hosts/1 ID-21500011
2        x.0.0.10        x.0.0.10        Infected-Hosts/1 ID-21500011
3        x.0.0.21        x.0.0.21        Infected-Hosts/1 ID-21500011
4        x.0.0.11        x.0.0.11        Infected-Hosts/1 ID-21500012
5        x.0.0.12        x.0.0.12        Infected-Hosts/1 ID-21500012
6        x.0.0.22        x.0.0.22        Infected-Hosts/1 ID-21500012
7        x.0.0.6         x.0.0.6         Infected-Hosts/1 ID-21500013
8        x.0.0.9         x.0.0.9         Infected-Hosts/1 ID-21500013
9        x.0.0.13        x.0.0.13        Infected-Hosts/1 ID-21500013
10       x.0.0.23        x.0.0.23        Infected-Hosts/1 ID-21500013
11       x.0.0.14        x.0.0.14        Infected-Hosts/1 ID-21500014
12       x.0.0.24        x.0.0.24        Infected-Hosts/1 ID-21500014
13       x.0.0.1         x.0.0.1         Infected-Hosts/1 ID-21500015
14       x.0.0.2         x.0.0.2         Infected-Hosts/1 ID-21500015
15       x.0.0.3         x.0.0.3         Infected-Hosts/1 ID-21500015
16       x.0.0.4         x.0.0.4         Infected-Hosts/1 ID-21500015
17       x.0.0.5         x.0.0.5         Infected-Hosts/1 ID-21500015
18       x.0.0.15        x.0.0.15        Infected-Hosts/1 ID-21500015
19       x.0.0.25        x.0.0.25        Infected-Hosts/1 ID-21500015
20       x.0.0.16        x.0.0.16        Infected-Hosts/1 ID-21500016
21       x.0.0.26        x.0.0.26        Infected-Hosts/1 ID-21500016
22       x.0.0.17        x.0.0.17        Infected-Hosts/1 ID-21500017
23       x.0.0.27        x.0.0.27        Infected-Hosts/1 ID-21500017
24       x.0.0.18        x.0.0.18        Infected-Hosts/1 ID-21500018
25       x.0.0.28        x.0.0.28        Infected-Hosts/1 ID-21500018
26       x.0.0.19        x.0.0.19        Infected-Hosts/1 ID-21500019
27       x.0.0.29        x.0.0.29        Infected-Hosts/1 ID-21500019
28       x.0.0.8         x.0.0.8         Infected-Hosts/1 ID-2150001a
29       x.0.0.20        x.0.0.20        Infected-Hosts/1 ID-2150001a
30       x.0.0.30        x.0.0.30        Infected-Hosts/1 ID-2150001a

Total number of matching entries: 30
```

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

The threat level of a host might decrease automatically if there have been no security events for that host for the period of one month. The month in question is a rolling window of time relative to the current time. The number and type of events seen over that month determine the threat level score of the host. A host might automatically be removed from the infected hosts list by the same process, if all malware events fall outside of that month long window.

If the manual resolution of a host sets the threat level to zero and another malware event occurs, the resolution event is ignored. The resulting threat score for the host once again takes into consideration all the suspicious events within the period of one month to determine the new threat score.

CHAPTER 8

Threat Sources

IN THIS CHAPTER

Threat Sources Overview

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

The Threat Sources page lists information of servers that have attempted to contact and compromise hosts on your network. A threat source is a centralized computer that issues commands to botnets (compromised networks of computers) and receives reports back from the botnets.

Benefits

Use Command and Control (C&C) feeds to:

- Add another layer of protection to your network, preventing the creation of botnets from within your network. Botnets gather sensitive information, such as account numbers or credit card information, and participate in distributed denial-of-service (DDoS) attacks.
- Prevent botnets from communicating with your network hosts to gather information or launch an attack.

You can allowlist threat sources from the details page. See "Threat Source Details" on page 91.

NOTE:

- C&C, GeoIP filtering and Domain Name System (DNS) feeds are only available with a Juniper ATP Cloud license. For a feature specific licensing information, see Software Licenses for ATP Cloud.

- At this time, C&C URL feeds are not supported with SSL forward proxy.
- The retention period for threat sources is 60 days.

The following information is available on this page.

Table 17: Threat Source Data Fields

Field	Definition
External Server	The IP address or hostname of the suspected threat source.
Blocked Via	Displays the custom feed name.
Highest Threat Level	The threat level of the threat source as determined by an analysis of actions and behaviors.
Count	The number of times hosts on the network have attempted to contact the threat server.
Country	The country where the threat source is located.
Last Seen	The date and time of the most recent threat source hit.
Action	The action taken on the communication For example: permitted, sinkhole, or blocked
Category	Displays the DNS feed category. The available options are custom, global, and allowlist.
DNS Record Type	Displays the query type of the DNS request. The supported DNS query types are A, AAAA, MX, CNAME, SRV, SRV NoErr, TXT, ANY, and so on.

RELATED DOCUMENTATION

Threat Source Details | 91

Host Details | 79

Threat Source Details

Access this page by clicking an **External Server** link from the **Threat Sources** page.

Use Threat Source Details page to view analysis information and a threat summary for the threat source. The following information is displayed for each threat source.

- Threat Summary (Location, Category, Host Name, and Time Seen)
- Total Hits
- Protocols and Ports(TCP and UDP)

For threat sources of type C&C, you can add the threat source to the allowlist or report it as a false positive to Juniper Networks from the Threat Source Details page.

For threat source of type DNS, you can only report the threat source as false positive to Juniper Networks.

Table 18: Options on the Threat Source Details Page (Upper Right Side of Page)

Button/Link	Purpose
Select **Option** > **Add to Whitelist**	Choose this option to add the threat source to the allowlist. **WARNING**: Adding a threat source to the allowlist automatically triggers a remediation process to update any affected hosts (in that organization) that have contacted the newly allowlisted threat source. All C&C events related to this allowlisted server will be removed from the affected hosts' events, and a host threat level recalculation will occur. If the host score changes during this recalculation, a new host event appears describing why it was rescored. (For example, "Host threat level updated after threat source 1.2.3.4 was cleared.") Additionally, the threat source will no longer appear in the list of threat source because it has been cleared. **NOTE**: You can also allowlist threat source from the **Configuration** > **Allowlists** page. See "Create Allowlists and Blocklists" on page 168 for details.

Table 18: Options on the Threat Source Details Page (Upper Right Side of Page) ***(Continued)***

Button/Link	Purpose
Select **Option** > **Report as False Positive**	Choose this option to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false positive or a false negative. Juniper will investigate the report, however, this does not change the verdict.

Under Time Range is a graph displaying the frequency of events over time. An event occurs when a host communicates to the threat source IP address (either sending or receiving data). You can filter this information by clicking the time-frame links: 1 day, 1 week, 1 month, Custom (select your own time-frame).

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

Table 19: Threat Source Contacted Host Data

Field	Definition
Client Host	The name of the host in contact with the threat source.
Client IP Address	The IP address of the host in contact with the threat source. (Click through to the Host Details page for this host IP.)
Threat Level at Time	The threat level of the threat source as determined by an analysis of actions and behaviors at the time of the event.
Status	The action taken by the device on the communication (whether it was permitted, sinkhole, or blocked).
Protocol	The protocol (TCP or UDP) the threat source used to attempt communication.
Source Port	The port the threat source used to attempt communication.
Device Name	The name of the device in contact with the threat source.

Table 19: Threat Source Contacted Host Data *(Continued)*

Field	Definition
Date/Time Seen	The date and time of the most recent threat source hit.
Username	The name of the host user in contact with the threat source.

Domains is a list of domains that the IP address has previously used at the time of suspicious events. If a threat source IP address is seen changing its DNS/domain name to evade detection, a list of the various DNS names used will be listed along with the dates in which these names were seen.

Table 20: Threat Source Associated Domains Data

Field	Definition
C & C Host	List of domains the destination IP addresses in the threat source events resolved to
Last Seen	The date and time of the most recent threat source server hit

Signatures is a list of the threat indicators associated with the IP address. The threat source blocked by the Juniper “Global Threat Feed” will show domains or signatures. (The “Blocked Via” column, under the threat source listing, shows whether a threat source IP address was found in the Juniper “Global Threat Feed” or in a different configured custom feed.)

Table 21: Threat Source Signature Data

Field	Definition
Name	The name or type of detected malware.
Category	Description of the malware and way in which it might have compromised a resource or resources.
Date	The date the malware was seen.

Certificates is a list of certificates associated with the threat source.

Table 22: Threat Source Certificate Data

Field	Definition
Certificate Hash	Displays the certificate hash of the threat source.
Date/Time Seen	The date and time when the certificate hash file was last updated.

RELATED DOCUMENTATION

- Threat Sources Overview | 89
- Host Details | 79
- Hosts Overview | 75

CHAPTER 9

Identify Hosts Communicating with Command and Control Servers

IN THIS CHAPTER

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 Firewall can intercept the traffic and perform an enforcement action based on real-time feed information from Juniper ATP Cloud. The Web UI identifies the C&C server IP address, its threat level, number of times the C&C server has been contacted, and so on

An **FP/FPN** button lets you report false positive or false negative for each C&C server listed. When reporting false negative, Juniper ATP Cloud will assign a C&C threat level equal to the global threat level threshold you assign in the misc configuration (**Configure > Misc Configuration**).

Juniper ATP Cloud blocks that host from communicating with the C&C server and can allow the host to communicate with other servers that are not on the C&C list depending on your configuration settings. The C&C threat level is calculated using a proprietary algorithm.

You can also use the `show services security-intelligence statistics` or `show services security-intelligence statistics profile` *`profile-name`* CLI commands to view C&C statistics.

```
user@root> show services security-intelligence statistics
Category Whitelist:
  Profile Whitelist:
    Total processed sessions: 0
    Permit sessions:          0
```

```
Category Blacklist:
  Profile Blacklist:
    Total processed sessions: 0
    Block drop sessions:      0
Category CC:
  Profile cc_profile:
    Total processed sessions: 5
    Permit sessions:          4
    Block drop sessions:      1
    Block close sessions:     0
    Close redirect sessions:  0
Category JWAS:
  Profile Sample-JWAS:
    Total processed sessions: 0
    Permit sessions:          0
    Block drop sessions:      0
    Block close sessions:     0
    Close redirect sessions:  0
Category Infected-Hosts:
  Profile hostintel:
    Total processed sessions: 0
    Permit sessions:          0
    Block drop sessions:      0
    Block close sessions:     0
```

In the following example, the C&C profile name is `cc_profile`.

```
user@root> show services security-intelligence statistics profile cc_profile
Category CC:
  Profile cc_profile:
    Total processed sessions: 5
    Permit sessions:          4
    Block drop sessions:      1
    Block close sessions:     0
    Close redirect sessions:  0
```

You can also use the `show services security-intelligence category detail category-name` *`category-name`* `feed-name` *`feed-name`* `count` *`number`* `start` *`number`* CLI command to view more information about the C&C servers and their threat level.

NOTE: Set both count and start to 0 to display all C&C servers.

For example:

```
user@root> show services security-intelligence category detail category-name CC
feed-name cc_url_data count 0 start 0
Category name   :CC
  Feed name     :cc_url_data
  Version       :20160419.2
  Objects number:24331
  Create time   :2016-04-18 20:43:59 PDT
  Update time   :2016-05-04 11:39:21 PDT
  Update status :Store succeeded
  Expired       :No
  Options       :N/A
  { url:http://g.xxxxx.net threat_level:9}
  { url:http://xxxx.xxxxx.net threat_level:9}
  { url:http://xxxxx.pw threat_level:2}
  { url:http://xxxxx.net threat_level:9}
  ...
```

RELATED DOCUMENTATION

- Configure the SRX Series Firewall to Block Outbound Requests to a C&C Host

CHAPTER 10

IoT Device Discovery and Classification

IN THIS CHAPTER

IoT Device Overview

IN THIS SECTION

Access this page from the Monitor menu.

Starting in Junos OS Release 22.1R1, Internet of Things (IoT) device discovery and classification is supported on the firewall.

The firewall identifies IoT devices based on the traffic flow, and streams the packet metadata to Juniper ATP Cloud. Juniper ATP Cloud identifies and classifies IoT devices. You can view the list of identified IoT devices on Juniper ATP Cloud portal and create threat feeds to enforce security policies across IoT traffic in the network.

For more information about IoT device discovery and classification on your firewall, see Security IoT User Guide.

Benefits of IoT

Knowledge of IoT devices in a network allows users or network administrators to better manage their network security and reduce IoT attack surface.

The following information is available on this page.

Table 23: Fields on the IoT Devices Page

Field	Description
Host	The hostname of the IoT device
IP	IP address of the IoT device
Category	The category which the IoT device belongs.
Manufacturer	The manufacturer of the IoT device
Model	The model number of the IoT device.
Operating System	The OS of the IoT device
Version	The software version of the IoT device.
Last Seen	The date and time of the most recent activity on IoT device.

Create Threat Feeds for IoT Devices

Use this page to add a new threat feed for IoT device. After creating the feed, you can enforce security policies across IoT traffic in the network. You can create a maximum of 64 feeds.

Review the "IoT Device Overview" on page 98 topic.

To add a new threat feed:

1. Select **Monitor > IoT Devices**.
   The IoT Devices page appears.
2. Select the desired filters based on the **Category, Manufacturer/Model, or OS/Version** and then click **Create Feed**.
   The Add New Feed page appears with the selected category.
3. Complete the configuration according to the guidelines provided in the Table 24 on page 100 table.

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

Table 24: Add New Feed Settings

Setting	Guideline
Feed Name	Enter a unique name for the threat feed. The feed name must begin with an alpha-numeric character and can include letters, numbers, and underscores; no spaces are allowed. The length is 8–63 characters.
Type	The content type (IP) of the feed is auto-selected. You cannot modify this field.
Data Source	The data source (IoT) of the feed is auto-selected. You cannot modify this field.
Time to Live	Enter the number of days for the required feed entry to be active. After the feed entry crosses the time to live (TTL) value, the feed entry is automatically removed. The available range is 1–365 days.

After you create a feed, the same feed will be available for configuration on the Junos CLI. You can also see the feeds in Adaptive Threat Profiling page on Juniper ATP Cloud portal. Navigate to **Configure > Adaptive Threat Profiling** to view the new feeds.

CHAPTER 11

Reverse Shell

IN THIS CHAPTER

Reverse Shell Overview

A reverse shell allows the attacker to bypass firewalls and other security mechanisms to open the ports to the target system.

When an attacker exploits a code execution vulnerability on the target system, they will run a script that starts a reverse shell session to the Command and Control (C&C) server. It gives them remote access to the compromised system. The attackers can run any command they want and obtain its output from the system. SRX Series Firewall will analyze the traffic pattern between the client and the server over a brief period to identify the reverse shell sessions. It will then take the configured remedial action.

Benefits of reverse shell detection

Helps you to detect shell attacks and prevent potential data thefts.

To access the Reverse Shell page, navigate to **Monitor** > **Reverse Shell**.

This page provides a list of destination IP addresses, destination ports, source IP addresses and source ports that were part of the reverse shell communication. See Figure 19 on page 102.

Figure 19: Reverse Shell

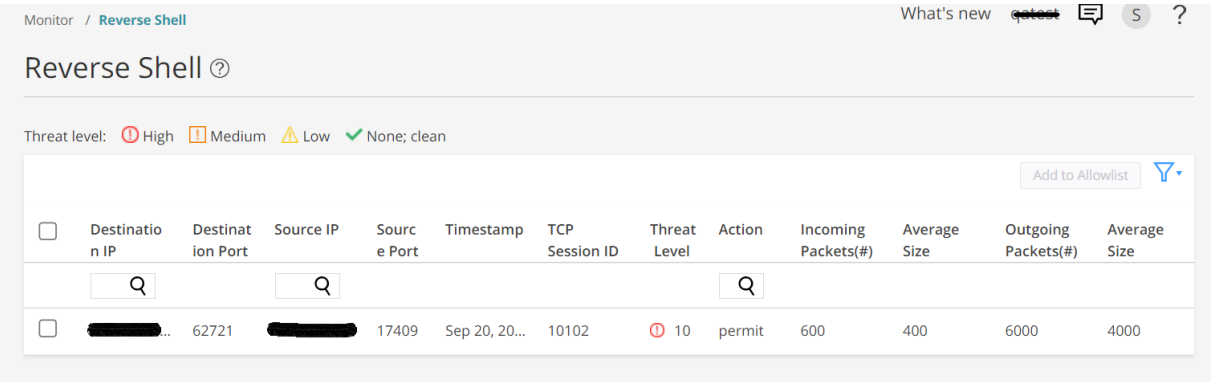


Table 25: Reverse Shell Page Data Fields

Field	Definition
Destination IP	The IP address of the attacker's C&C server
Destination Port	The port of the attacker's C&C server
Source IP	The IP address of the target system in reverse shell session.
Source Port	The port the attackers used to attempt reverse shell communication.
Timestamp	Date and time the reverse shell session is started.
TCP Session ID	The session ID assigned to the attacker's C&C server
Threat Level	The threat level of the attacker's C&C server based on the analysis.
Action	The action taken on the reverse shell session: permit or block.
Incoming Packets(#)	The number of incoming packets to the target system.
Average Size	The average size of the incoming packets.

Table 25: Reverse Shell Page Data Fields *(Continued)*

Field	Definition
Outgoing Packets(#)	The number of outgoing packets from the target system.
Average Size	The average size of the outgoing packets.

You can select and add the destination IP addresses to the allowlists if they are not malicious. To add the destination IP address to the allowlists:

1. Select **Monitor** > **Reverse Shell**.

   The Reverse Shell page appears.

2. Select the destination IP address that you want to add to the allowlists and then click **Add to Allowlist**.

   A pop-up appears asking you to confirm the selection.

3. Click **Yes**.

   The selected destination IP address is added to the allowlists.

For information about configuring the reverse shell detection on SRX Series Firewalls, see Juniper Advanced Threat Prevention Administrator Guide.

RELATED DOCUMENTATION

Allowlist and Blocklist Overview | 163

CHAPTER 12

Files

IN THIS CHAPTER

HTTP File Download Overview

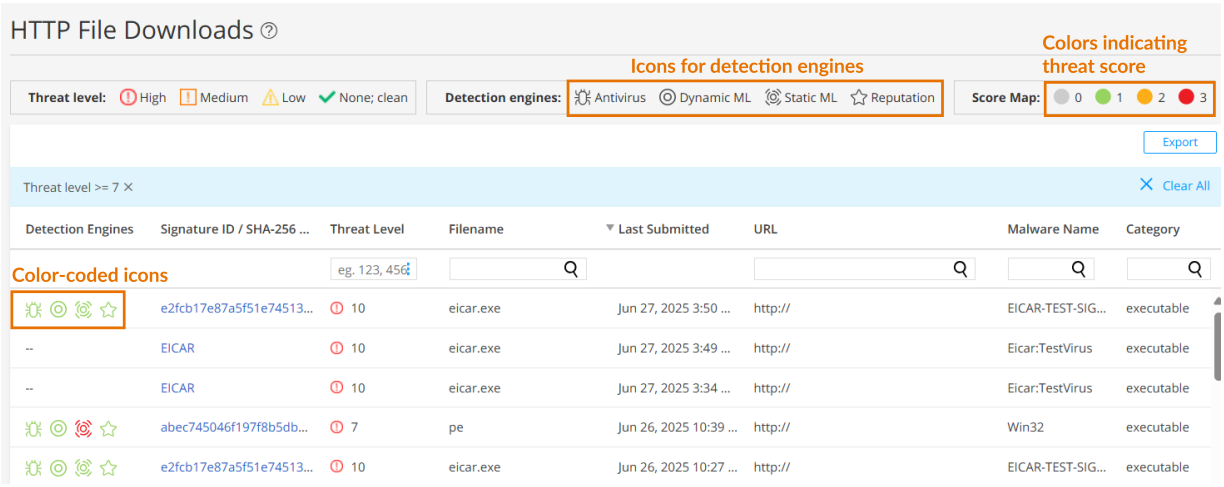
Access the HTTP File Download page from the **Monitor > Files > HTTP File Downloads** menu.

Benefits of viewing HTTP File Downloads

- Allows you to view a compiled list of suspicious downloaded files all in one place, including the signature, threat level, URL, and malware type.
- Allows you to filter the list of downloaded files by individual categories.

Export Data—Click the Export button to download file scanning data to a CSV file. You are prompted to narrow the data download to a selected time-frame.

Figure 20: HTTP File Downloads



The following information is available on this page.

Table 26: HTTP Scanning Data Fields

Field	Definition
Detection Engine	Displays color-coded icons representing the confidence levels of various detection engines in identifying threats. For more information more detection engines, see Table 27 on page 106. The color codes signify the following threat severities: • Red—High threat severity • Orange—Moderate threat severity • Green—Low threat severity • Gray—No threats detected To view the threat severity score assigned by each detection engine, hover over the icons.

Table 26: HTTP Scanning Data Fields *(Continued)*

Field	Definition
Signature ID / SHA-256 / ML Hit	If applicable, the Signature ID uniquely identifies the signature that is triggered for this detection; otherwise, the SHA-256 file hash is displayed. • If a full file is uploaded to the Juniper ATP Cloud, a hash of the file is displayed in this column. • If the file is blocked, and the transfer is interrupted on the SRX Series Firewall, a Signature ID is displayed. • If the file is detected by the inline machine learning (ML)-based threat detection engine on the SRX Series Firewall, "N/A" is displayed in this column.
Threat Level	The threat score. Click the three vertical dots at the top of the column to filter the information in the page by threat level.
Filename	The name of the file, including the extension
Last Submitted	The time and date of the most recent file scan
URL	The URL from which the file originated
Malware Name	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

Table 27: Detection Engines

Detection Engines	Description
Antivirus	• Commercial antivirus • Commercial cloud multi-antivirus engine

Table 27: Detection Engines *(Continued)*

Detection Engines	Description
Dynamic ML	• Juniper's sandbox-based ML • Juniper's cloud sandbox-based ML
Static ML	• Juniper's cloud ML antivirus • Juniper's ML engines using file attributes • Commercial cloud static antivirus
Reputation	File hash reputation

RELATED DOCUMENTATION

- Email Attachments Scanning Overview | **131**
- File Scanning Limits | **123**
- HTTP File Download Details | **107**
- Manual Scanning Overview | **122**
- Hosts Overview | **75**
- Host Details | **79**
- Statistics Overview | **143**

HTTP File Download Details

IN THIS SECTION

- File Summary | **110**
- Static Analysis | **111**
- Behavior Analysis | **113**

To access this page, navigate to **Monitor** > **Files** > **HTTP File Downloads**. Click the **Signature ID** link to go to the File Download Details page.

Use this page to view general, static analysis, behavior analysis, network activity, and malware behavior summaries for the downloaded file. This page is divided into several sections:

Table 28: Links on the HTTP File Download Details Page

Button/Link	Purpose
Report False Positive	Click this button to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report, however, this investigation does not change the verdict. If you want to make a correction (mark system as clean), you must do it manually.

Table 28: Links on the HTTP File Download Details Page *(Continued)*

Button/Link	Purpose
Download STIX Report	When there is a STIX report available, a download link appears on this page. Click the link to view gathered, open-source threat information, such as blocklisted files, addresses and URLs. STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties. STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing and consuming. Juniper ATP Cloud uses this information as well as other sources. This occurs automatically. There is no administrator configuration required for STIX. STIX reports will vary. View a sample report at the bottom of this page. **NOTE**: Juniper ATP Cloud can also share threat intelligence. You can control what threat information is shared from the Threat Sharing page. See "Configure Threat Intelligence Sharing" on page 220.
Download Zipped Files	(When available) Click this link to download the quarantined malware for analysis. The link allows you to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the General tab in the Juniper ATP Cloud UI for the file in question.
Download PDF Report	Click this link to download a detailed report on the file in question. The report provides details on file threat level, protocol seen, and file category and size. It also includes client IP address, username, and additional information, if available. This data is provided in a formatted PDF with a TOC.

The top of the page provides a quick view of the following information (scroll to the right in the UI to see more boxes):

- **Threat Level**—This is the threat level assigned (0-10), This box also provides the filename, and threat category.
- **Top Indicators**—In this box, you will find the malware name, the signature it matches, antivirus state, and the IP address/URL from which the file originated.

- **Prevalence**—This box provides information about how often this malware has been seen, how many individual hosts on the network downloaded the file, and the protocol used.

File Summary

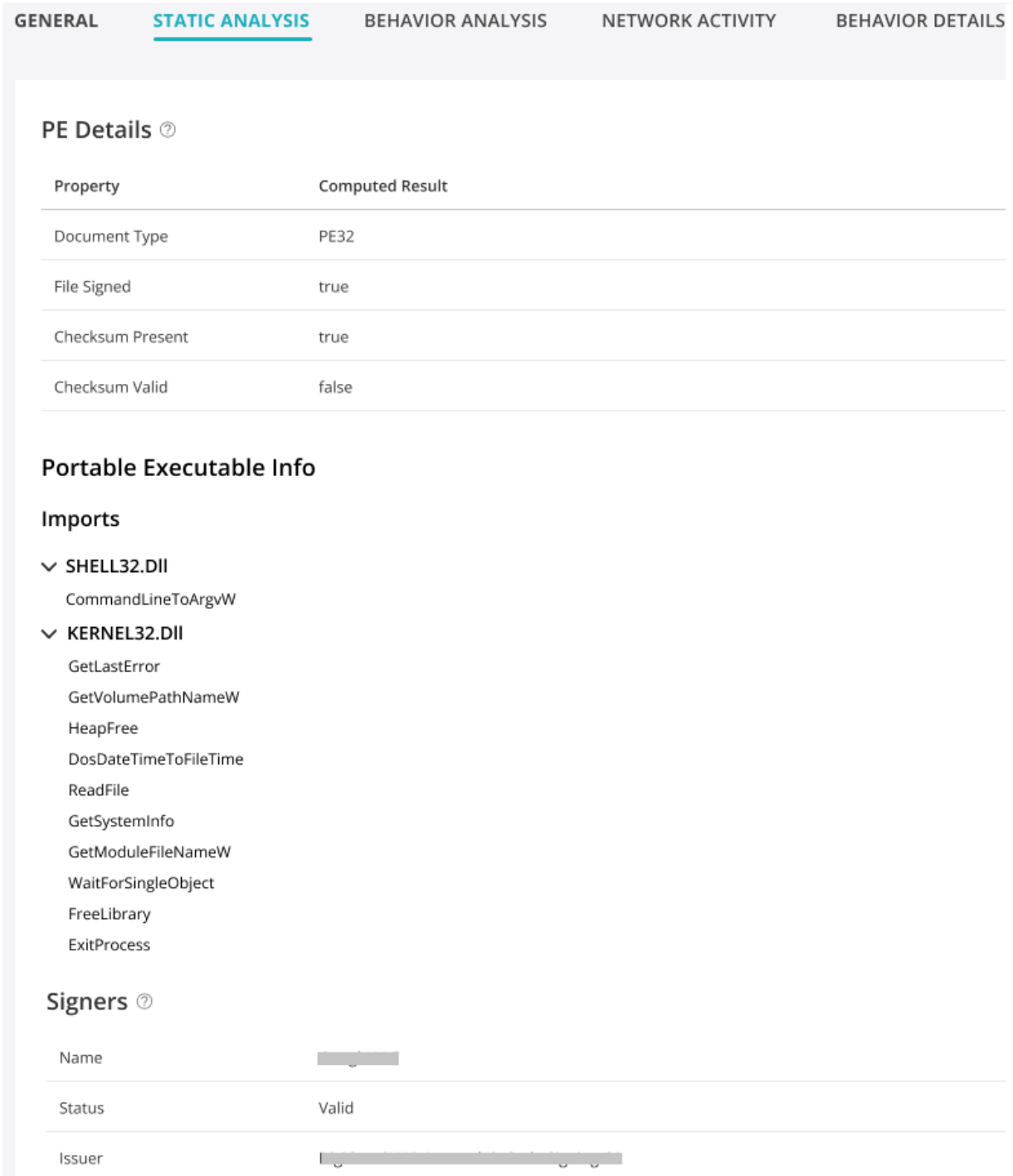
Table 29: General Summary Fields

Field	Definition
Threat Level	This is the assigned threat level 0-10. 10 is the most malicious.
Global Prevalence	How often this file has been seen across different customers.
Last Scanned	The time and date of the last scan to detect the suspicious file
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe, wordmui.msi.
Category	The type of file Examples: PDF, executable, document
Size	The size of the downloaded file.
Platform	The target OS of the file Example: Win32
Malware Name	If possible, Juniper ATP Cloud determines the name of the malware.
Type	If possible, Juniper ATP Cloud determines the type of threat. Example: Trojan, Application, Adware.
Strain	If possible, Juniper ATP Cloud 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.

Static Analysis

Juniper ATP Cloud provides static file information such as document type, certificate details, signer information and so on for explaining potential sample capabilities.

Figure 21: Statistic analysis information



Behavior Analysis

Juniper ATP Cloud provides network behavioral analysis and machine learning (ML) to determine if an encrypted or non-encrypted connection is benign or malicious. Please note that the SSL proxy is needed to decrypt the traffic for detection.

Behavior analysis tab displays the file execution behavior trends in a radar chart with malware categories or behaviors on each axis. This data helps us better identify the category of a malware and map that category to a severity.

The malware priority is classified into low, medium, and high.

In Figure 22 on page 113 the radar chart on the left contains the probability of the sample that it belongs to one of these mentioned malware types. The shape point towards one specific malware type, in this case, Trojan. This indicates that the sample's malware type is most probably Trojan. Note that this graph Figure 22 on page 113 may not exist for some possibly malicious samples after sandboxing. In the chart, green indicates clean in that category, orange indicates suspicious in that category, and red indicates malicious malware in that category.

Figure 22: Malware Category Information

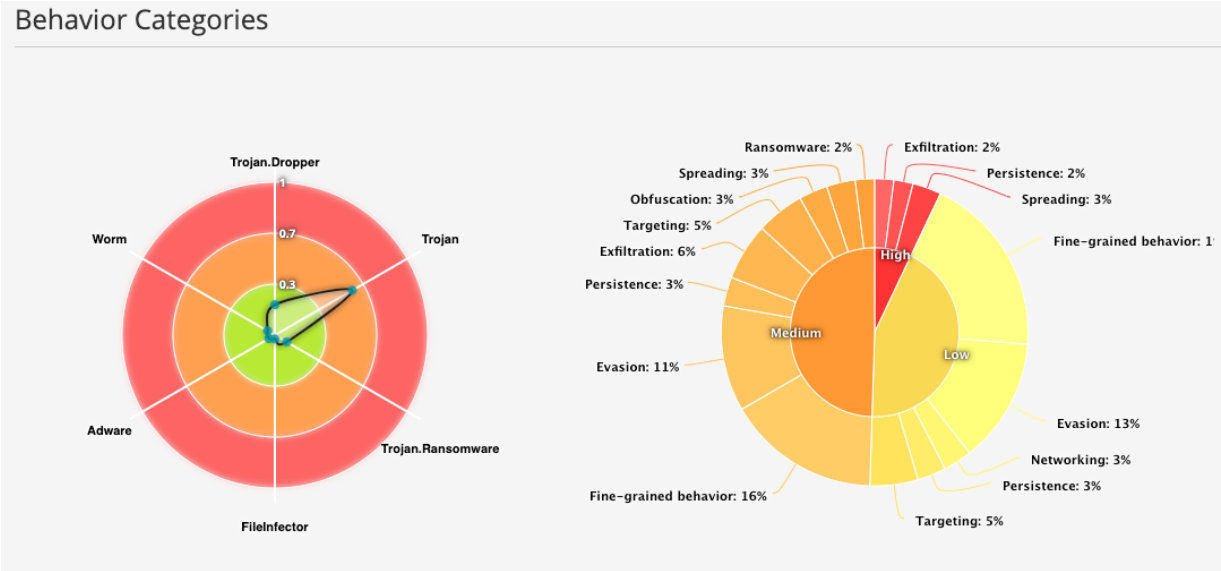


Table 30: Behavior Analysis Fields

Behavior Category	Sample Behavior Definition
Targeting	Checks volume information

Table 30: Behavior Analysis Fields *(Continued)*

Behavior Category	Sample Behavior Definition
Fine-grained Behavior	Contains code to communicate with device drivers. Contains code to delete services. Memory allocated in system DLL range.
Obfuscation	Utilizes known code obfuscation techniques.
Evasion	Contains code to detect VMs. Contains large amount of unused code (likely obfuscated code). Contains code to determine API calls at runtime.
Persistence	Modifies registry keys to run application during startup.
Networking	Memory or binary contains Internet addresses.

HTTP Downloads

This section displays the list of hosts that have downloaded the suspicious file. Click the **IP address** to be taken to the Host Details page for this host. Click the **Device Serial number** to be taken to the Devices page. From there you can view device versions and version numbers for the Juniper ATP Cloud configuration, including profile, allowlist, and blocklist versions. You can also view the malware detection connection type for the device: telemetry, submission, or C&C event.

Network Activity

In the Network Activity section, you can view information in the following tabs:

- **Contacted Domains**—If available, lists any domains that were contacted while executing the file in the Juniper ATP Cloud 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.

Behavior Details

The behavior details tab displays information about suspicious activities and process details captured during the behavioral analysis. For example, if malware drops an executable file and starts a new process, these details are displayed under the behavioral details tab. Screenshots of behavioral analysis windows are also shown for the malware analysis that occurred inside the sandbox. This helps you determine whether the file is malware. If the analyzed file is ransomware, you might see its ransom message or other information displayed during the analysis in the screenshot.

Please note that the screenshots are available only for the newly analyzed files.

Sample STIX Report

Figure 23: Sample STIX Report

```
<?xml version="1.0"?>
- <stix:STIX_Package version="1.2" id="example:Package-afbc14e2-b192-4ea0-848f-0a95aaea6cb3" xmlns:WinProcessObj="http://cybox.mitre.org/objects#WinProcessObject-2"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:WinRegistryKeyObj="http://cybox.mitre.org/objects#WinRegistryKeyObject-2" xmlns:stix="http://stix.mitre.org/stix-1"
xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1" xmlns:WinThreadObj="http://cybox.mitre.org/objects#WinThreadObject-2" xmlns:example="http://example.com"
xmlns:stixCommon="http://stix.mitre.org/common-1" xmlns:cybox="http://cybox.mitre.org/cybox-2" xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
xmlns:ttp="http://stix.mitre.org/TTP-1" xmlns:xlink="http://www.w3.org/1999/xlink" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2" xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
xmlns:ProcessObj="http://cybox.mitre.org/objects#ProcessObject-2" xmlns:indicator="http://stix.mitre.org/Indicator-2" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  - <stix:STIX_Header>
      <stix:Description>IOCs for sample id: a9c097d0f6392897ff87764d43ac9ad4b60078f7062325b7798909e484f3f1af</stix:Description>
    </stix:STIX_Header>
  - <stix:Indicators>
    - <stix:Indicator id="example:indicator-92000f82-82b0-45bf-9ac7-bf4566c1c93d" xsi:type="indicator:IndicatorType" timestamp="2017-10-09T20:31:25.918941+00:00">
        <indicator:Title>File Indicator(s) for sample:a9c097d0f6392897ff87764d43ac9ad4b60078f7062325b7798909e484f3f1af</indicator:Title>
        <indicator:Description>An indicator containing File observable(s)</indicator:Description>
      - <indicator:Observable id="example:Observable-987ee5c7-6c56-414c-a696-f3199d5aa0fb">
        - <cybox:Object id="example:File-4f1c86c5-725b-4d44-b19e-e1787dc05c28">
          - <cybox:Properties xsi:type="FileObj:FileObjectType">
            - <FileObj:Hashes>
              - <cyboxCommon:Hash>
                  <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0">MD5</cyboxCommon:Type>
                  <cyboxCommon:Simple_Hash_Value>b941993d05adf34dc9b7d35fe3f0ae61</cyboxCommon:Simple_Hash_Value>
                </cyboxCommon:Hash>
              - <cyboxCommon:Hash>
                  <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA1</cyboxCommon:Type>
                  <cyboxCommon:Simple_Hash_Value>e70f1bb911ee60ef6e7aa2c423eaa5a04d17e709</cyboxCommon:Simple_Hash_Value>
                </cyboxCommon:Hash>
              - <cyboxCommon:Hash>
                  <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA256</cyboxCommon:Type>
                  <cyboxCommon:Simple_Hash_Value>a9c097d0f6392897ff87764d43ac9ad4b60078f7062325b7798909e484f3f1af</cyboxCommon:Simple_Hash_Value>
                </cyboxCommon:Hash>
              - <cyboxCommon:Hash>
                  <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0">SHA512</cyboxCommon:Type>
                  <cyboxCommon:Simple_Hash_Value>1afc3d6e068c8e3bb617726a0ecdec428da99c874ef2f1c98538651b6d537bf5e8d00a0e2c49b2d20740146c9ef5f77
                </cyboxCommon:Hash>
              </FileObj:Hashes>
            </cybox:Properties>
          </cybox:Object>
        </indicator:Observable>
```

RELATED DOCUMENTATION

File Scanning Limits | 123
HTTP File Download Overview | 104
Manual Scanning Overview | 122
Hosts Overview | 75

Signature Details

IN THIS SECTION

To access the malware signature details page, go to.

- **Monitor** > **Files** > **HTTP File Download**
- **Monitor** > **Files** > **Email Attachments**
- **Monitor** > **Files** > **SMB File Download**

Click **Signature ID** link to go to the Signature Details page.

Use the Signature Details page to view the malware signature details. The malware signatures are provided by Juniper ATP Cloud to the SRX Series Firewalls. When an SRX Series Firewall detects a malware file, the device can block the file immediately based on these malware signatures and the advanced anti-malware (AAMW) policy that is configured on the SRX Series Firewall. The malware signatures are shared with the SRX Series Firewalls whenever there is an update in Juniper ATP Cloud. For each malware signature hit, the SRX Series Firewall provides the malware signature hit report to Juniper ATP Cloud.

This page is divided into several sections:

- **Report False Positive**—Click this button to launch a new screen to send a report to Juniper Networks, informing if the report is a false positive or a false negative. Juniper will investigate the report, however, this investigation does not change the verdict. If you want to make a correction (mark system as clean) you must do it manually.
- **Threat Level**—This is the threat level assigned (0-10). This box also provides the signature filename, threat category and the action taken.
- **Prevalence**—Provides information about how often this malware has been seen, how many individual hosts on the network downloaded the file, and the protocol used.

Table 31: Signature Summary

Field	Description
General	Displays signature information of the associated file
Static Analysis	Displays information about file type or file source associated with the signature. The file types that are supported are PE/DLL, doc, docx Office - old format, office - new format, PDF, RTF.
Behavior Analysis	Displays the behavior analysis for the file associated with the signature
Network Activity	Displays the network activity for the file associated with the signature
Behavior Details	Displays the behavior data for the file associated with the signature

Signature Summary

The General tab displays the details for the file associated with the signature. Please note that this file might not be the exact file seen in your network. It is the file used to generate the signature that your file has triggered. The details include file category, timestamp of when the signature was created, statistics about how often the signature was hit, the current status of the signature (enabled/disabled), and so on.

Figure 24: General Information

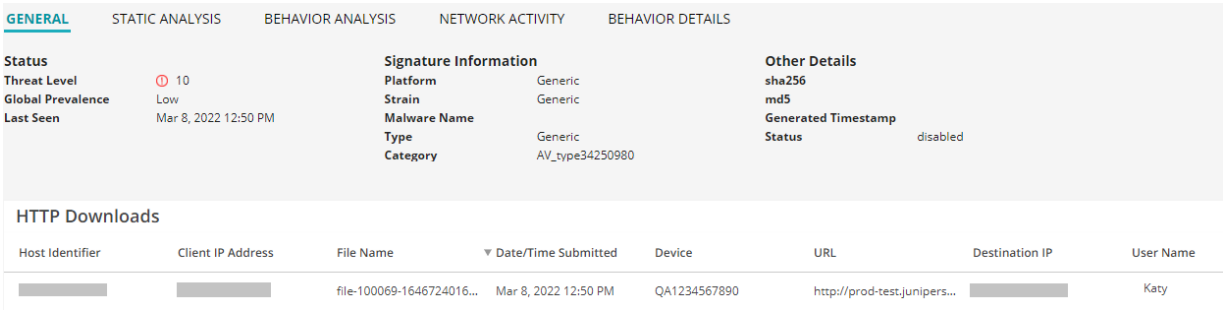


Table 32: General Summary Fields

Field	Definition
Status	
Threat Level	This is the assigned threat level 0-10. 10 is the most malicious.
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
Signature Information	
Platform	The target OS of the file Example: Win32
Strain	If possible, Juniper ATP Cloud determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio
Malware Name	If possible, Juniper ATP Cloud determines the name of the malware.
Type	If possible, Juniper ATP Cloud determines the type of threat. Example: Trojan, Application, Adware
Category	If possible, Juniper ATP Cloud determines the category of threat.

Table 32: General Summary Fields *(Continued)*

Field	Definition
Other Details	
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.
Generated Timestamp	The time when the signature was generated.
Status	The current status of the signature (enabled/disabled)

HTTP Downloads

This section displays the list of hosts that have downloaded the suspicious file. Click the **IP address** to be taken to the Host Details page for this host. Click the **Device Serial number** to be taken to the Devices page. From there you can view device versions and version numbers for the Juniper ATP Cloud configuration, including profile, allowlist, and blocklist versions. You can also view the malware detection connection type for the device: telemetry, submission, or C&C event.

Static Analysis

Juniper ATP Cloud provides static analysis and machine learning (ML) to determine if the file is potentially malicious.

Behavior Analysis

Juniper ATP Cloud provides network behavioral analysis and ML to analyze the behavior of the sample, including the connections it makes to various hosts. However, the analysis is still for primarily sandboxed sample analysis and not for connection analysis.

Behavior analysis tab displays the file execution behavior trends in a radar chart with malware categories or behaviors on each axis. This data helps us better identify the category of a malware and map that category to a severity.

The malware priority is classified into low, medium, and high.

Figure 25: Behavior analysis

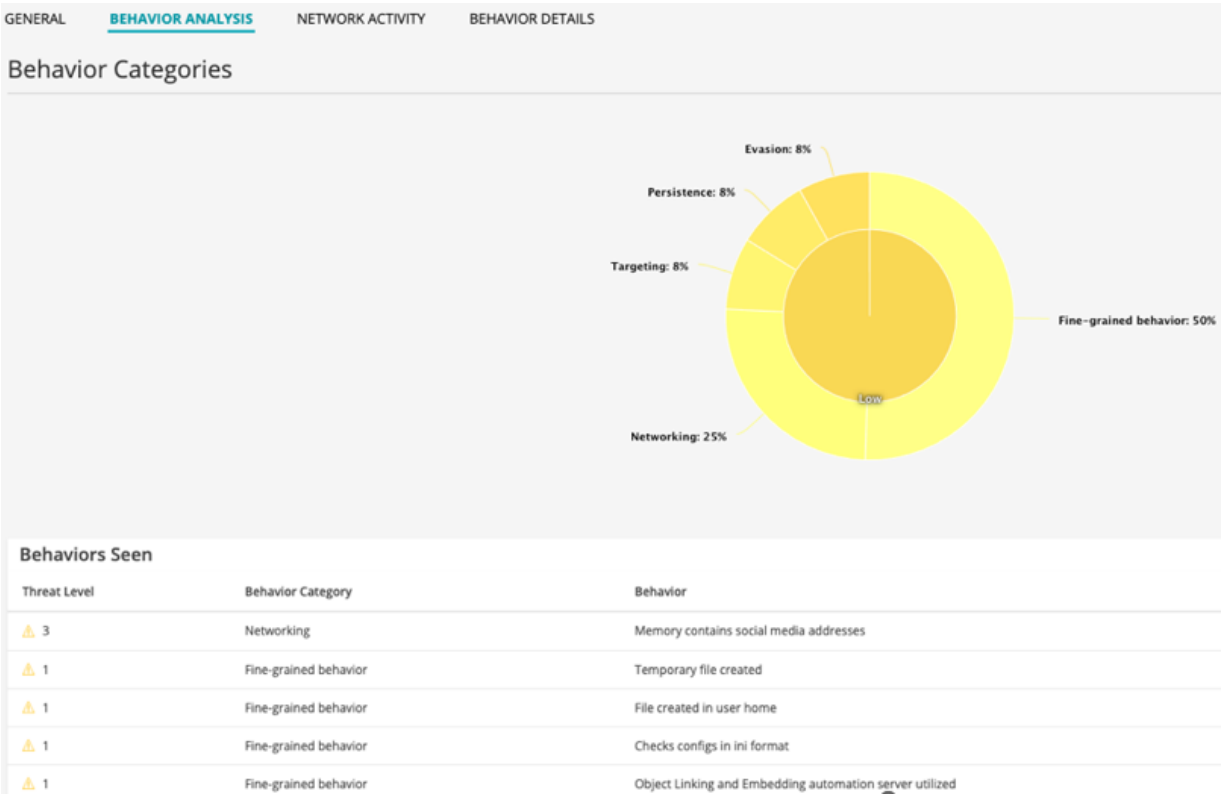


Table 33: Behavior Analysis Fields

Behavior Category	Sample Behavior Definition
Targeting	Checks volume information
Fine-grained Behavior	Contains code to communicate with device drivers. Contains code to delete services. Memory allocated in system DLL range
Obfuscation	Utilizes known code obfuscation techniques.

Table 33: Behavior Analysis Fields *(Continued)*

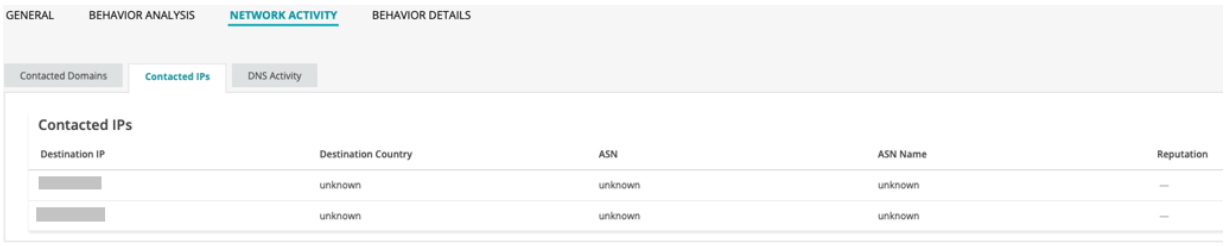
Behavior Category	Sample Behavior Definition
Evasion	Contains code to detect VMs. Contains large amount of unused code (likely obfuscated code). Contains code to determine API calls at runtime.
Persistence	Modifies registry keys to run application during startup.
Networking	Memory or binary contains Internet addresses.

Network Activity

In the Network Activity section, you can view information in the following tabs:

- **Contacted Domains**—If available, lists any domains that were contacted while executing the file in the Juniper ATP Cloud 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.

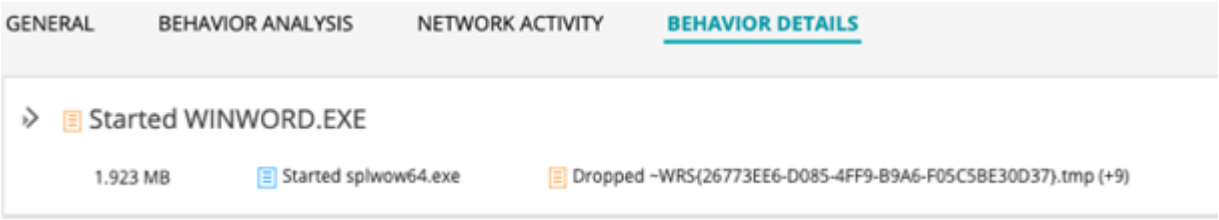
Figure 26: Network activity



Behavior Details

This section displays the behavior data for the file associated with the signature.

Figure 27: Behavior details



Manual Scanning Overview

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

If you suspect a file is suspicious, you can manually upload it to the cloud for scanning and evaluation. Click the **Manual Upload** button to browse to the file you want to upload. The file can be up to 32 MB.

Benefits of Manually Scanning Files

- Allows you to investigate files that weren't filtered by existing blocklists.
- Provides all file analysis data that accompanies known suspicious files, such as behavior analysis and network activity.

There is a limit to the number of files administrators can upload for manual scanning. File uploads are limited by organization (across all users in an organization) in a 24-hour period. You can upload two files per each active device enrolled and 10 files per each premium-licensed device in your account. For example, if you have two Juniper ATP Cloud premium-licensed SRX Series Firewalls and one other SRX Series Firewall, Juniper ATP Cloud will allow a maximum of 22 files to be allowed in a 24-hour window. For more licensing information, see Software Licenses for ATP Cloud.

NOTE: You must have an SRX Series Firewall registered with Juniper ATP Cloud in order to use the manual file scanning feature.

Table 34: Files Data Fields

Field	Definition
File Signature	A unique identifier located at the beginning of a file that provides information about 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 file scan
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 | **75**
- HTTP File Download Overview | **104**
- HTTP File Download Details | **107**
- Email Attachments Scanning Overview | **131**
- Email Attachments Scanning Details | **134**

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 and protocols such as HTTP, IMAP and SMTP.

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

Table 35 on page 124 lists the maximum number of files per day that you can submit to the Juniper ATP Cloud for inspection.

Table 35: Maximum Number of Files Per Day Per Device Submitted to Cloud for Inspection

Perimeter Device	Standard License (Files per Day)	Premium License (Files per Day)
SRX300	100	500
SRX320	100	500
SRX340	200	1,000
SRX345	300	2,000
SRX380	300	3,000
SRX550	500	5,000
SRX1500	2,500	10,000
SRX1600	2,500	10,000
SRX2300	2,500	15,000
SRX4100	3,000	20,000
SRX4120	3,000	20,000
SRX4200	3,000	35,000

Table 35: Maximum Number of Files Per Day Per Device Submitted to Cloud for Inspection *(Continued)*

Perimeter Device	Standard License (Files per Day)	Premium License (Files per Day)
SRX4300	4,000	45,000
SRX4600	5,000	60,000
SRX4700	5,000	60,000
SRX5400	5,000	50,000
SRX5600	5,000	70,000
SRX5800	5,000	100,000
vSRX (10 mbps)	25	200
vSRX (100 mbps)	200	1,000
vSRX (1000 mbps)	2,500	10,000
vSRX (2000 mbps)	2,500	10,000
vSRX (4000 mbps)	3,000	20,000

For more licensing information, see Software Licenses for ATP Cloud.

RELATED DOCUMENTATION

- HTTP File Download Overview | **104**
- Email Attachments Scanning Overview | **131**
- Manual Scanning Overview | **122**

SMB File Download Overview

Access the SMB File Download page from the **Monitor > Files > SMB File Downloads** menu.

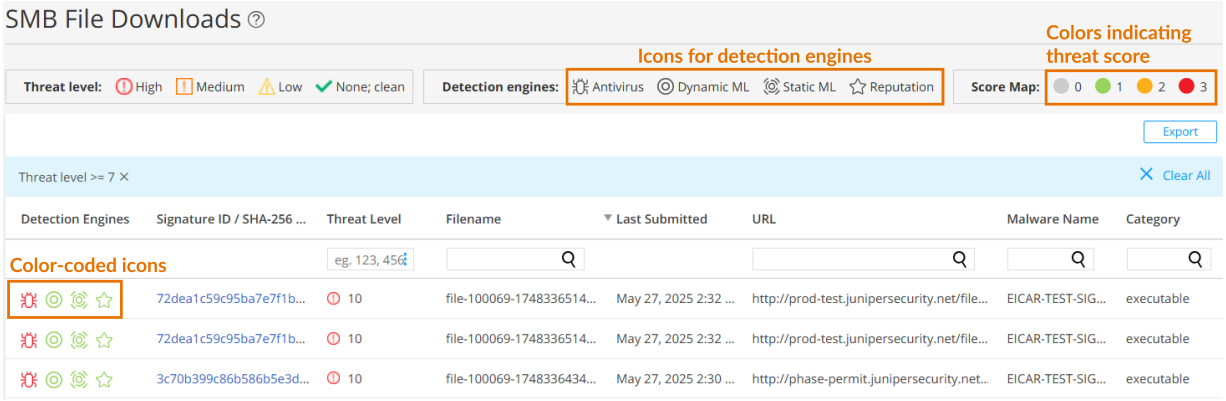
The Server Message Block (SMB) protocol enables applications or users to access files and other resources on a remote server.

Benefits of viewing SMB File Downloads

- Allows you to view a compiled list of suspicious downloaded files all in one place, including the signature, threat level, URL, and malware type.
- Allows you to filter the list of downloaded files by individual categories.

Export Data—Click the Export button to download file scanning data to a CSV file. You are prompted to narrow the data download to a selected time-frame.

Figure 28: SMB File Downloads



The following information is available on this page.

Table 36: SMB Scanning Data Fields

Field	Definition
Detection Engine	Displays color-coded icons representing the confidence levels of various detection engines in identifying threats. For more information about detection engines, see Table 27 on page 106. The color codes signify the following threat severities: • Red—High threat severity • Orange—Moderate threat severity • Green—Low threat severity • Gray—No threats detected To view the threat severity score assigned by each detection engine, hover over the icons.
Signature ID / SHA-256 / ML Hit	If applicable, the Signature ID uniquely identifies the signature that is triggered for this detection; otherwise, the SHA-256 file hash is displayed. • If a full file is uploaded to the Juniper ATP Cloud, a hash of the file is displayed in this column. • If the file is blocked, and the transfer is interrupted on the SRX Series Firewall, a Signature ID is displayed. • If the file is detected by the inline machine learning (ML)-based threat detection engine on the SRX Series Firewall, "N/A" is displayed in this column.
Threat Level	The threat score. Click the three vertical dots at the top of the column to filter the information in the page by threat level.
Filename	The name of the file, including the extension
Last Submitted	The time and date of the most recent file scan
URL	The URL from which the file originated.

Table 36: SMB Scanning Data Fields *(Continued)*

Field	Definition
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."
Category	The type of file Examples: PDF, executable, document

RELATED DOCUMENTATION

- SMB File Download Details | **128**
- Hosts Overview | **75**
- Host Details | **79**

SMB File Download Details

IN THIS SECTION

To access this page, navigate to **Monitor** > **Files** > **SMB File Download**. Click the **Signature ID** link to go to the SMB File Download 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 37: Links on the SMB File Download Details Page

Button/Link	Purpose
Report False Positive	Click this button to launch a new screen which lets you send a report to Juniper Networks, informing Juniper of a false position or a false negative. Juniper will investigate the report, however, this does not change the verdict.
Download STIX Report	When there is a STIX report available, a download link appears on this page. Click the link to view gathered, open-source threat information, such as blocklisted files, addresses and URLs. STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties. STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing and consuming. Juniper ATP Cloud uses this information as well as other sources. This occurs automatically. There is no administrator configuration required for STIX. STIX reports will vary. View a sample report at the bottom of this page. **NOTE**: Juniper ATP Cloud can also share threat intelligence. You can control what threat information is shared from the Threat Sharing page. See "Configure Threat Intelligence Sharing" on page 220.
Download Zipped File	(When available) Click this link to download the quarantined malware for analysis. The link allows you to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the General tab in the Juniper ATP Cloud UI for the file in question.
Download PDF Report	Click this link to download a detailed report on the file in question. The report includes file threat level, protocol seen, file category and size, client IP address and username, and much more information, if available. This data is provided in a formatted PDF with a TOC.

The top of the page provides a quick view of the following information (scroll to the right in the UI to see more boxes):

- **Threat Level**—This is the threat level assigned (0-10), This box also provides the filename and threat category.
- **Top Indicators**—In this box, you will find the signature match for the filename, and the antivirus details.
- **Prevalence**—This box provides information about how often this malware has been seen, how many individual hosts on the network downloaded the file, and the protocol used.

File Summary

Table 38: General Summary Fields

Field	Definition
General	
Threat Level	This is the assigned threat level 0-10. 10 is the most malicious.
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 Information	
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe, wordmui.msi.
Category	The type of file Examples: PDF, executable, document
Size	The size of the downloaded file.
Platform	The target OS of the file Example: Win32
Malware Name	If possible, Juniper ATP Cloud determines the name of the malware.

Table 38: General Summary Fields *(Continued)*

Field	Definition
Type	If possible, Juniper ATP Cloud determines the type of threat. Example: Trojan, Application, Adware.
Strain	If possible, Juniper ATP Cloud determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio
Other Details	
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.

SMB Downloads

This is a list of hosts that have downloaded the suspicious file. Click the **Host Identifier** link to be taken to the Host Details page for this host.

RELATED DOCUMENTATION

SMB File Download Overview | 126

Hosts Overview | 75

Host Details | 79

Email Attachments Scanning Overview

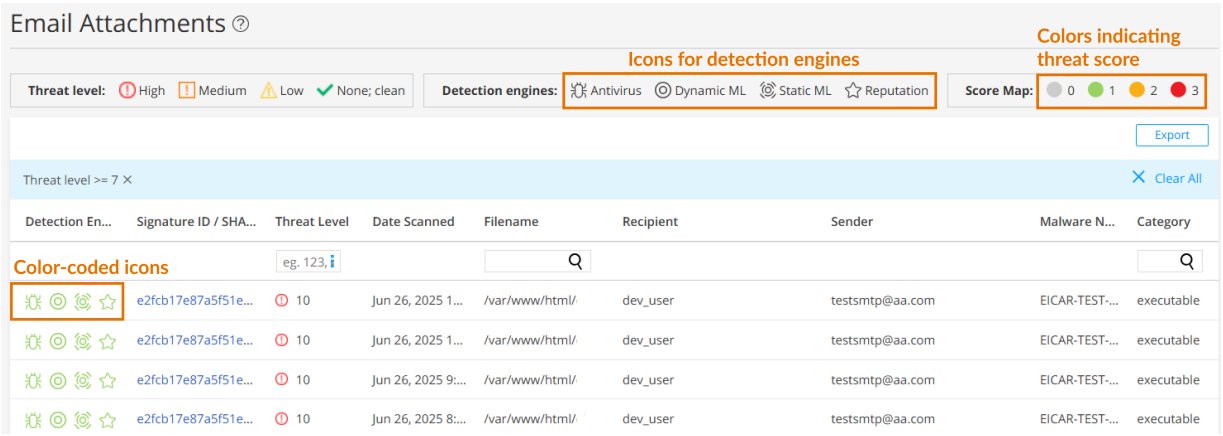
Access the Email Attachments page from the **Monitor > Files > Email Attachments** menu.

Benefits of Viewing Scanned Email Attachments

- Allows you to view a compiled list of suspicious email attachments all in one place, including the file hash, threat level, filename, and malware type.
- Allows you to filter the list of email attachments by individual categories.

Export Data—Click the Export button to download file scanning data to a CSV file. You are prompted to narrow the data download to a selected time-frame.

Figure 29: Email Attachments



The following information is available on this page.

Table 39: Email Attachments Scanning Data Fields

Field	Definition
Detection Engine	Displays color-coded icons representing the confidence levels of various detection engines in identifying threats. For more information about detection engines, see Table 27 on page 106. The color codes signify the following threat severities: • Red—High threat severity • Orange—Moderate threat severity • Green—Low threat severity • Gray—No threats detected To view the threat severity score assigned by each detection engine, hover over the icons.

Table 39: Email Attachments Scanning Data Fields *(Continued)*

Field	Definition
Signature ID / SHA-256 / ML Hit	If applicable, the Signature ID uniquely identifies the signature that is triggered for this detection; otherwise, the SHA-256 file hash is displayed. • If a full file is uploaded to the Juniper ATP Cloud, a hash of the file is displayed in this column. • If the file is blocked, and the transfer is interrupted on the SRX Series Firewall, a Signature ID is displayed. • If the file is detected by the inline machine learning (ML)-based threat detection engine on the SRX Series Firewall, "N/A" is displayed in this column.
Threat Level	The threat score. Click the three vertical dots at the top of the column to filter the information in the page by threat level.
Date Scanned	The date and time the file was scanned.
Filename	The name of the file, including the extension
Recipient	The email address of the intended recipient
Sender	The email address of the sender
Malware Name	The type of malware found
Status	Indicates whether the file was blocked or permitted.
Category	The type of file Examples: PDF, executable, document

RELATED DOCUMENTATION

Email Attachments Scanning Details | 134

Email Attachments Scanning Details

IN THIS SECTION

To access this page, navigate to **Monitor** > **Files** > **Email Attachments**. Click the **Signature ID** link to go to the Files 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 investigation does not change the verdict. If you want to make a correction (mark system as clean) you must do it manually.

Download STIX Report—

When there is a STIX report available, a download link appears on this page. Click the link to view gathered, open-source threat information, such as blocklisted files, addresses and URLs. STIX (Structured Threat Information eXpression) is a language used for reporting and sharing threat information using TAXII (Trusted Automated eXchange of Indicator Information). TAXII is the protocol for communication over HTTPS of threat information between parties.

STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing and consuming. Juniper ATP Cloud uses this information as well as other sources. This occurs automatically. There is no administrator configuration required for STIX.

NOTE: Juniper ATP Cloud can also share threat intelligence. You can control what threat information is shared from the Threat Sharing page. See "Configure Threat Intelligence Sharing" on page 220.

Download Zipped Files—(When available) Click this link to download the quarantined malware for analysis. The link allows you to download a password-protected zipped file containing the malware. The password for the zip file is the SHA256 hash of the malware exe file (64 characters long, alpha numeric string) shown in the General tab in the Juniper ATP Cloud 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 40: General Summary Fields

Field	Definition
Threat Level	This is the assigned threat level 0-10. 10 is the most malicious.
Action Taken	The action taken based on the threat level and host settings: block or permit.
Global Prevalence	How often this file has been seen across different customers.
Last Scanned	The time and date of the last scan to detect the suspicious file.
File Name	The name of the suspicious file. Examples: unzipper-setup.exe, 20160223158005.exe,, wordmui.msi.

Table 40: General Summary Fields *(Continued)*

Field	Definition
Category	The type of file. Examples: PDF, executable, document.
File Size	The size of the downloaded file.
Platform	The target operating system of the file. Example. Win32
Malware Name	If possible, Juniper ATP Cloud determines the name of the malware.
Type	If possible, Juniper ATP Cloud determines the type of threat. Example: Trojan, Application, Adware.
Strain	If possible, Juniper ATP Cloud determines the strain of malware detected. Example: Outbrowse.1198, Visicom.E, Flystudio.
Other Details	
sha256 and md5	One way to determine whether a file is malware is to calculate a checksum for the file and then query to see if the file has previously been identified as malware.

In the Network Activity section, you can view information in the following tabs:

NOTE: This section will appear blank if there has been no network activity.

- **Contacted Domains**—If available, lists any domains that were contacted while executing the file in the Juniper ATP Cloud 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 | **104**
- HTTP File Download Details | **107**
- Email Attachments Scanning Overview | **131**
- Manual Scanning Overview | **122**
- Quarantined Emails Overview | **138**

CHAPTER 13

E-mails

IN THIS CHAPTER

Quarantined Emails Overview

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

The Quarantined Emails 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 and adding these emails to the blocklist.

The following information is available from the Summary View:

Table 41: Emails 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	Total number of emails scanned during the chosen time-frame and then categorizes them into blocked, quarantined, released, and permitted emails.
Malicious Email Count	A graphical representation of emails, organized by time, with lines for blocked emails, quarantined and not released emails, and quarantined and released emails.

Table 41: Emails Summary View *(Continued)*

Field	Description
Emails Scanned	A graphical representation of emails, organized by time, with lines for total emails, and emails with one or more attachments.
Email Classification	Another graphical view of classified emails, organized by percentage of blocked emails, quarantined and not released emails, and quarantined and released emails.

The following information is available from the Details View:

Table 42: Emails Details 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 Juniper ATP Cloud quarantine portal and preview the email.
Date	The date the email was received.
Malicious Attachment	Click the attachment name to go to the Juniper ATP Cloud file scanning page where you can view details about the attachment.
Size	The size of the attachment in KB
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.

Table 42: Emails Details View *(Continued)*

Field	Description
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 blocklist
- Add sender to blocklist
- Release

RELATED DOCUMENTATION

Emails Overview | 180

Emails: Configure SMTP | 182

Create Allowlists and Blocklists | 168

HTTP File Download Overview | 104

Blocked Attachments Overview

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

The Blocked Attachments 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 and adding these emails to the blocklist.

The following information is available from the Summary View:

Table 43: Emails 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.

Table 43: Emails Summary View *(Continued)*

Field	Description
Malicious Email Count	Total number of malicious emails scanned during the chosen time-frame and then categorized them into the following: • Blocked • Blocked and not allowed • Quarantined and allowed
Emails Scanned	A graphical representation of all scanned emails, organized by date

The following information is available from the Detail View:

Table 44: Emails 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 Juniper ATP Cloud quarantine portal and preview the email.
Date	The date the email was received.
Malicious Attachment	Click the attachment name to go to the Juniper ATP Cloud file scanning page where you can view details about the attachment.
Size	The size of the attachment in KB
Threat Score	The threat score of the attachment, 0-10, with 10 being the most malicious.

Table 44: Emails 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:

- Unblock Attachment for Selected User(s)
- Unblock Attachment for All Users

RELATED DOCUMENTATION

Emails: Configure IMAP | **186**

Emails Overview | **180**

CHAPTER 14

Statistics

IN THIS CHAPTER

Statistics Overview

NOTE: Statistics support is available starting in Junos OS 17.4R1.

Access this page from the **Monitor** > **Statistics** > **Web Protocols** or **Email Protocols** menu.

The statistics page provides comprehensive monitoring information of devices for a variety of activities, including the number of web and e-mail files scanned or blocked per protocol. It also offers a counter reset capability.

Benefits of Statistics

- Exposes monitoring data in the Juniper ATP Cloud web portal that was previously only accessible from the SRX Series Firewall through CLI.
- Centralizes valuable monitoring data in one place, facilitating the ability to put events in context against other events for a more comprehensive view of the network.

Reset button—When you select the check box for a device and click Reset, it clears the counter to zeros for that device and protocol. This reset applies only to the information displayed on the web portal.

NOTE: In a chassis cluster environment (both active/passive, active/active), each node shares the statistics data separately. Both the node details are displayed separately in the ATP Cloud UI.

For the Devices listed on this page, you can view the following information for Web Protocols by selecting the HTTP tab and the HTTPS tab.

Table 45: Statistics Data for Web Protocols

Web Protocols	Available Data
HTTP and HTTPS	Host Name—Click on the hostname to open the statistics details page for the device. The Device Details page contains: • Device Information—You can view the device name, model number, serial number, OS version, and submission state.
	Device Serial Number
	Total Scanned
	Blocked
	Permitted
	Ignored
	Blocklist hits
	Allowlist hits
	Last Reset This is the time when the device counter was last reset to zeros. Note that the reset applies only to the information that is displayed on the web portal.

For the Devices listed on this page, you can view the following information for Email Protocol by selecting the tabs that correspond to SMTP, SMTPS, IMAP, and IMAPS.

Table 46: Statistics Data for Email Protocols

Email Protocols	Available Data
SMTP and SMTPS IMAP and IMAPS	Host Name—Click on the hostname to open the statistics details page for the device. The Device Details page contains: • Device Information—You can view the device name, model number, serial number, OS version, and submission state.
	Device Serial Number
	Total Scanned
	Blocked
	Permitted
	Ignored
	Blocklist hits
	Allowlist hits
	Last Reset This is the time when the device counter was last reset to zeros. Note that the reset applies only to the information that is displayed on the web portal.

RELATED DOCUMENTATION

Statistics Details | **146**

HTTP File Download Overview | **104**

Email Attachments Scanning Overview | **131**

Statistics Details

To access this page, navigate to **Monitor** > **Statistics** > **Web Protocols** or **Email Protocols** > **<Protocol> tab** > **<Device Name>**. Click the device name link for any available device to access the details page.

Use this page to view device information. See the table below for a list of data points available on this page.

Table 47: Device Information

Field	Definition
Device Name	Hostname of the SRX Series firewall
Model Number	SRX Series firewall model number
Serial Number	SRX Series firewall serial number
OS Version	SRX Series firewall Junos OS version
Submission State	Allowed or Paused This status indicates whether the device can submit files to Juniper ATP Cloud or if it has reached its daily limit. See "File Scanning Limits" on page 123.

RELATED DOCUMENTATION

Statistics Overview | 143

HTTP File Download Details | 107

Email Attachments Scanning Details | 134

CHAPTER 15

DNS

IN THIS CHAPTER

DNS DGA Detection Overview

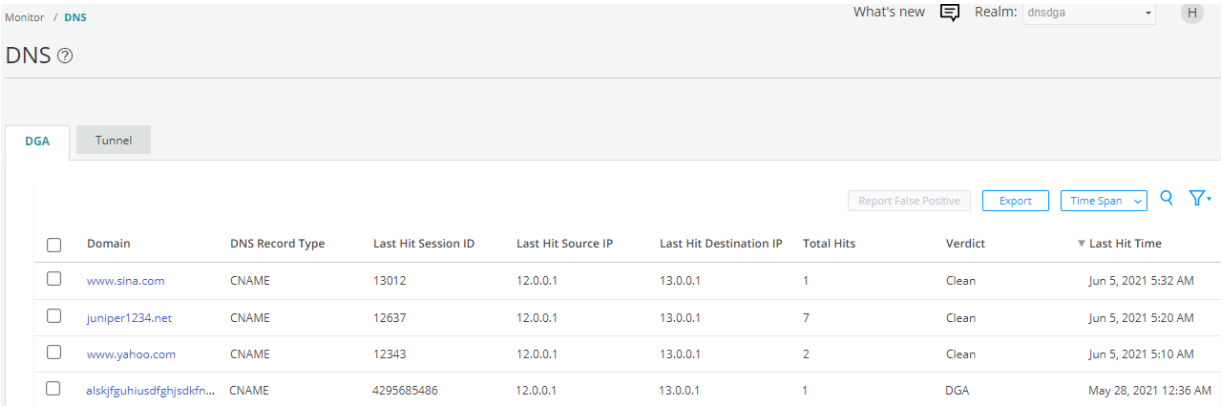
Domain Name System (DNS) Domain Generation Algorithm (DGA) generates random domain names that are used as rendezvous points with potential C&C servers. DNS DGA detection uses machine learning (ML) models as well as known pre-computed DGA domain names and provides domain verdicts, which helps inline blocking and sinkholing of DNS queries on SRX Series Firewalls.

Juniper ATP Cloud provides an ML-based DGA detection model. SRX Series Firewall acts as a collector of security metadata and streams the metadata to Juniper ATP Cloud for DGA analysis. We use both ATP Cloud service and security-metadata-streaming framework to conduct DGA Inspection in the cloud.

DNS DGA detection is available only with Juniper ATP Cloud license. For feature specific licensing information, see Software Licenses for ATP Cloud

To view DNS DGA detections, log in to Juniper ATP Cloud Web portal and navigate to **Monitor > DNS**. The DGA detections are displayed as shown in Figure 30 on page 148

Figure 30: DNS DGA Page



To enable DNS DGA detections on SRX Series Firewalls, see Juniper Advanced Threat Prevention Cloud Administration Guide.

NOTE: Domain Name System Security Extensions (DNSSEC) and Extension Mechanisms for DNS (EDNS) queries are not supported. By default, these queries are dropped.

DNS Tunnel Detection Overview

IN THIS SECTION

DNS Tunneling is a cyber-attack method that encodes the data of other programs or protocols in DNS queries and responses. It indicates that DNS traffic is likely to be subverted to transmit data of another protocol or malware beaconing.

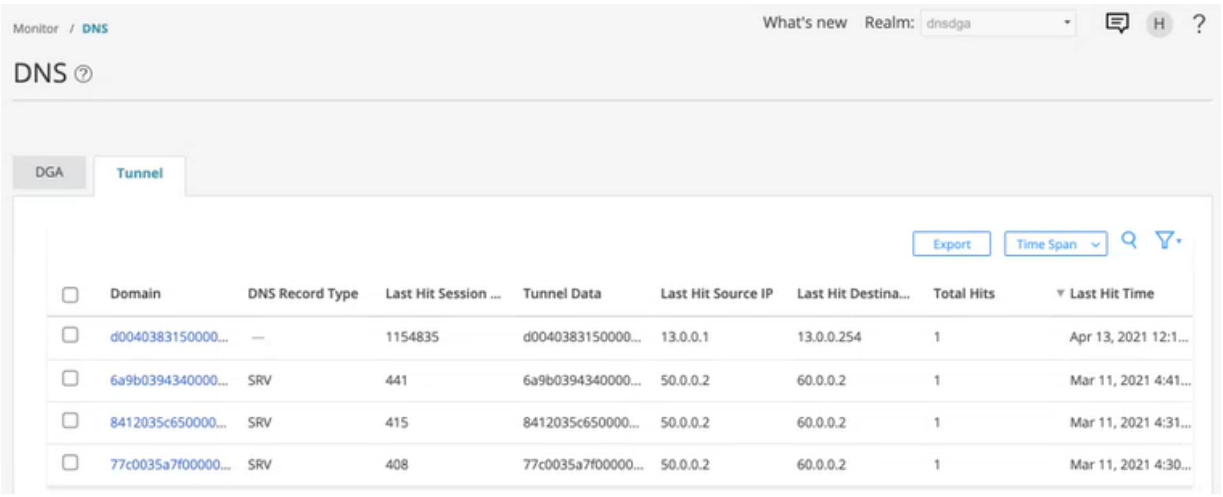
When a DNS packet is detected as tunneled, the SRX Series Firewall can take permit, deny or sinkhole action.

DNS Tunneling detection is available only with ATP Cloud license. For feature specific licensing information, see Software Licenses for ATP Cloud.

SRX Series Firewall exports the tunneling metadata to Juniper ATP Cloud. To view the DNS tunneling detections, log in to Juniper ATP Cloud Web portal and navigate to **Monitor > DNS**. Click on the **Tunnel**

tab to view the DNS tunnel detections as shown in Figure 31 on page 149. You can click on a domain name to view more details of the hosts that have contacted the domain.

Figure 31: DNS Tunnel Page



To enable DNS tunnel detections on SRX Series Firewalls, see Juniper Advanced Threat Prevention Cloud Administration Guide.

DNS Tunneling Procedure

Here's how DNS tunneling works:

1. A cyber attacker registers a malicious domain, for example, “badsite.com”.
2. The domain’s name server points to the attacker’s server, where DNS Tunneling malware program is running.
3. DNS Tunnel client program running on the infected host generates DNS requests to the malicious domain.
4. DNS resolver routes the query to the attacker’s command-and-control server.
5. Connection is established between victim and attacker through DNS resolver.
6. This tunnel can be used to exfiltrate data or for other malicious purposes.

DNS DGA and Tunneling Detection Details

IN THIS SECTION

To access this page, click **Monitor** > **DNS**.

You can view details about DNS DGA and tunnel detections.

DGA

You can perform the following action in the DGA tab:

- View details about the DGA-based detections. See Table 48 on page 150.
- View the threat sources if there is a C&C hit for a domain. Click domain name with DGA verdict to view the threat sources.
- Report false positives. Choose this option to send a report to Juniper Networks, informing a false positive. Juniper will investigate the report; however, this does not change the verdict.
- Export DGA detections as a CSV file to view and analyze the exported DGA detections as needed. You can either export all detections at once or for a specific timespan.
- Select the time span to view the DGA detections for a specific period.

Table 48: Fields on the DGA Tab

Field	Description
Domain	Displays the domain name where DGA hit occurs.

Table 48: Fields on the DGA Tab *(Continued)*

Field	Description
DNS Record Type	Displays the DNS record type. Example: A (Host address), CNAME (Canonical name for an alias), SRV (location of service), and so on. • A— DNS record is used to point a domain or subdomain to an IP address. • CNAME—DNS record is used to point a domain or subdomain to another hostname. • SRV—DNS record is used to point a domain or subdomain to a service location.
Last Hit Session ID	Displays the ID of the most recent domain hit.
Last Hit Source IP	Displays the source IP address of the most recent domain hit.
Last Hit Destination IP	Displays the destination IP address of the most recent domain hit.
Total Hits	Displays the total number of hits on the domain.
Verdict	Displays the confirmed DGA verdict provided by ATP Cloud. • Clean • DGA
Last Hit Time	Displays the date and time of the most recent domain hit.

Tunnel

Use the Tunnel tab to monitor the DNS tunneling metadata provided by SRX Series Firewalls. Table 49 on page 152 displays the DNS tunneling metadata.

You can perform the following action in the Tunnel tab:

- View details about the DNS tunneling metadata provided by SRX Series Firewalls. Table 49 on page 152 displays the DNS tunneling metadata.
- Export DNS Tunnel detections as a CSV file to view and analyze the exported DNS tunneling detections as needed. You can either export all detections at once or for a specific timespan.
- Select the time span to view the DNS tunneling detections for a specific period.
- View detailed information about a DNS tunnel. Click on a domain name. See Table 50 on page 153
- Download PCAP from the DNS Tunnel page. Select a client and click **Download PCAP** to download the packet capture details and view more information about the network.

Table 49: Fields on the Tunnel Tab

Field	Description
Domain	Displays the domain name
DNS Record Type	Displays the DNS record type. Example: A (Host address), CNAME (Canonical name for an alias), SRV (location of service), and so on. • A— DNS record used to point a domain or subdomain to an IP address. • CNAME—DNS record used to point a domain or subdomain to another hostname. • SRV—DNS record used to point a domain or subdomain to a service location.
Last Hit Session ID	Displays the session ID of the most recent domain hit.
Tunnel Data	Displays the tunnel information shared by SRX Series Firewall

Table 49: Fields on the Tunnel Tab *(Continued)*

Field	Description
Last Hit Source IP	Displays the source IP address of the most recent domain hit.
Last Hit Destination IP	Displays the destination IP address of the most recent domain hit.
Total Hits	Displays the total number of sessions that were hit.
Last Hit Time	Displays the date and time of the most recent domain hit.

Table 50: Fields on the DNS Tunnel page

Field	Description
Client IP Address	Displays the IP address of the host that has contacted the DNS domain.
Device Name	Displays the name of the SRX Series Firewall in contact with the DNS domain
Incoming Bytes	Displays the number of incoming bytes to the DNS tunnel.
Outgoing Bytes	Displays the number of outgoing bytes from the DNS tunnel.
Last Seen	The date and time of the most recent DNS tunnel hit.

NOTE: DNS DGA and tunnel detection is supported on Junos OS 21.2R1 and later releases.

CHAPTER 16

Encrypted Traffic Insights

IN THIS CHAPTER

Encrypted Traffic Insights Overview and Benefits

IN THIS SECTION

Access this page from the **Monitor** > **Encrypted Traffic** menu.

Encrypted traffic insights helps you to detect malicious threats that are hidden in encrypted traffic without intercepting and decrypting the traffic.

Benefits of encrypted traffic insights

- Monitors network traffic for threats without breaking the encryption of the traffic, thereby adhering to data privacy laws.
- Erases the need for additional hardware or network changes to set up and manage the network:
  - The SRX Series Firewall provides the required metadata (such as known malicious certificates and connection details) and connection patterns to ATP Cloud.
  - The ATP Cloud provides behavior analysis and machine learning (ML) capabilities.
- Provides greater visibility and policy enforcement over encrypted traffic without requiring resource-intensive SSL decryption:

  - Based on the network behaviors analyzed by ATP Cloud, the network connections are classified as malicious or benign.

- Adds a layer of protection beyond traditional information security solutions to help organizations reduce and manage risk.
- Ensures no latency as we do not decrypt the traffic.

Table 51 on page 155 lists the information that is available on the Encrypted Traffic Insights page.

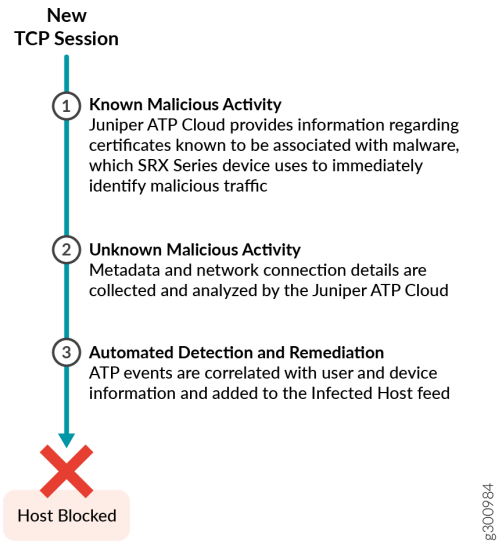
Table 51: Encrypted Traffic Insights

Field	Guideline
External Server IP	The IP address of the external server
External Server Hostname	The hostname of the external server
Highest Threat Level	The threat level on the external server based on encrypted traffic insights.
Count	The number of times hosts on the network has attempted to contact this server.
Country	The country where the external server is located.
Last Seen	The date and time of the most recent external server hit.
Category	Additional category information known about this server, for example, botnets, malware, and so on

Encrypted Traffic Insights and Detection

The encrypted traffic insights combines rapid response and network analysis (both static and dynamic) to detect and remediate malicious activity hidden in encrypted sessions. Figure 32 on page 156 shows the staged approach for encrypted traffic insights.

Figure 32: Encrypted Traffic Insights and Detection



Workflow

This section provides the topology and workflow to perform encrypted traffic insights.

Figure 33 on page 157 shows the logical topology of encrypted traffic insights workflow.

Figure 33: Topology for encrypted traffic insights

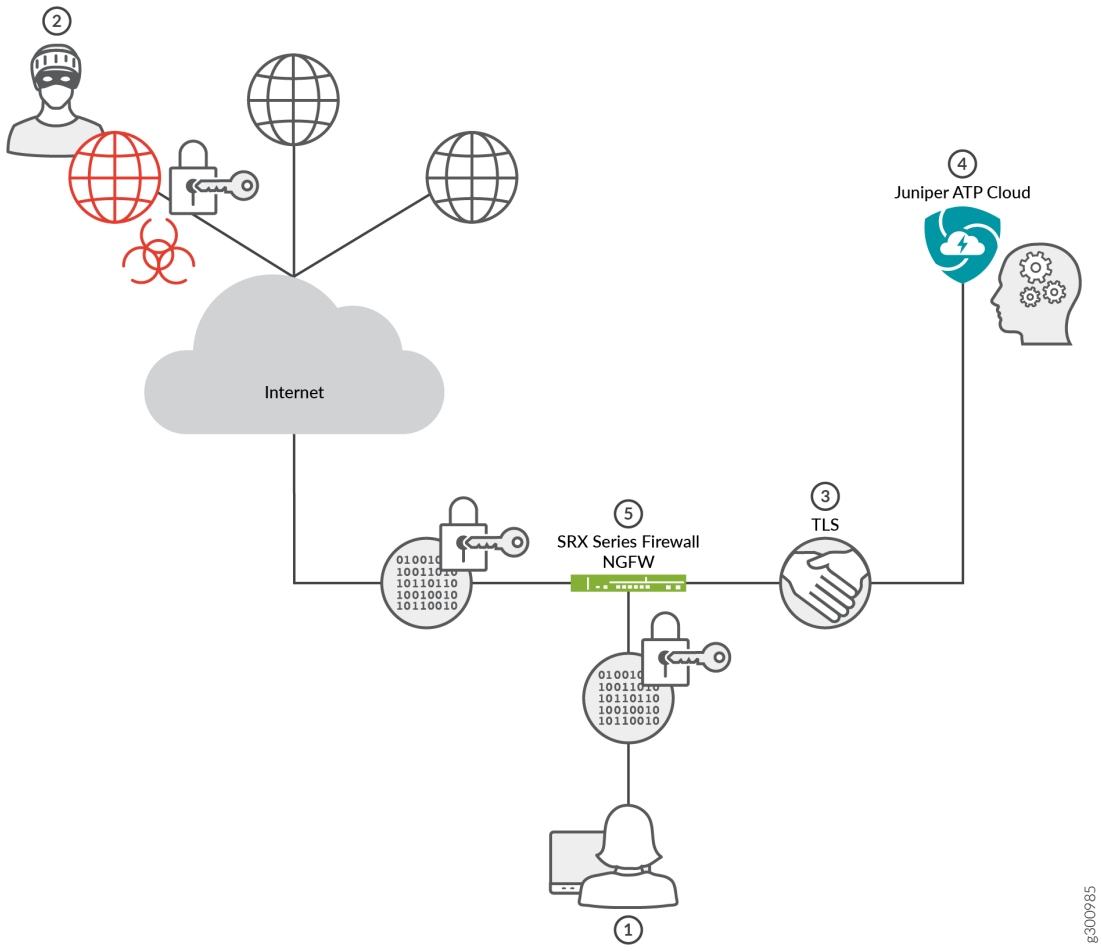


Table 52: Encrypted Traffic Insights Workflow

Step	Description
1	A client host, who is located behind an SRX Series Firewall requests a file to be downloaded from the Internet.
2	The SRX Series Firewall receives the response from the Internet. The SRX Series Firewall extracts the server certificate from the session and compares its signature with the blocklist certificate signatures. If a match occurs, then connection is blocked. **NOTE**: The Juniper Networks ATP Cloud feed keeps the SRX Series Firewall up to date with a feed of certificates associated with known malware sites.

Table 52: Encrypted Traffic Insights Workflow *(Continued)*

Step	Description
3	The SRX Series Firewall collects the metadata and connection statistics and sends it to the ATP Cloud for analysis.
4	The ATP Cloud performs behavioral analysis to classify the traffic as benign or malicious.
5	If a malicious connection is detected, the threat score of the host is recalculated. If the new score is above the threshold, then the client host is added to infected host list, The client host might be blocked based on policy configurations on SRX Series Firewalls.

For information about enabling encrypted traffic insights on SRX Series Firewalls, see Juniper Advanced Threat Prevention Cloud Administration Guide.

Encrypted Traffic Insights Details

To access this page, navigate to **Monitor** > **Encrypted Traffic**. Click any of the **External Server IP** address link.

Use Encrypted Traffic Insights Details page to view analysis information and a threat summary for the external server. The following information is displayed for each server:

- Total Hits
- Threat Summary (Location, Category, Time last seen)
- Ports and protocols used

The encrypted traffic insights details page is divided into several sections:

Table 53 on page 159 lists the actions that you can perform on this page. You can perform these actions using the options that are available on the upper right corner of page.

Table 53: Options on the Encrypted Traffic Insights Details Page

Button/Link	Purpose
Select **Option** > **Add to Whitelist**	Choose this option to allowlist the server from encrypted traffic insights based detections. **NOTE**: You can also allowlist the servers from the **Configure** > **Whitelists** > **ETA** page.
Select **Option** > **Report False Positive**	Choose this option to send a report to Juniper Networks, informing Juniper of a false positive. Juniper will investigate the report; however, this does not change the verdict.

Under Time Range is a graph displaying the frequency of events over time. An event occurs when a host communicates to the external server IP address (either sending or receiving data). You can filter this information by clicking the time frame links: 1 day, 1 week, 1 month, Custom (select your own time-frame).

Hosts is a list of hosts that have contacted the external server. Table 54 on page 159 lists the information provided in this section.

Table 54: External Server Contacted Host Data

Field	Definition
Client Host	The name of the host in contact with the external server
Client IP Address	The IP address of the host in contact with the external server (Click through to the Host Details page for this host IP address.)
Threat Level at Time	The threat level of the external server as determined by an analysis of actions and behaviors at the time of the event.
Status	The action taken by the device on the communication (whether it was permitted or blocked). **NOTE**: At this point of time, encrypted traffic insights only detects malicious threats but does not block it. Actions such as blocking is handled by features such as infected hosts based on the host threat score and customer policies.

Table 54: External Server Contacted Host Data *(Continued)*

Field	Definition
Protocol	The protocol (HTTPS) the external server used to attempt communication.
Source Port	The port the external server used to attempt communication.
Uploaded	Number of bytes uploaded to the server.
Downloaded	Number of bytes downloaded from the server.
Device Name	The name of the SRX Series Firewall in contact with the external server
Date/Time Seen	The date and time of the most recent external server hit.
Username	The name of the host user in contact with the external server

Select a client host and click **Download packet** to download the packet capture details and view more information about the network/SSL traffic.

Domains is a list of domains that the IP address has previously used at the time of suspicious events. If an external IP address is seen changing its DNS/domain name to evade detection, a list of the various names used will be listed along with the dates in which they were seen.

Table 55: External Server Associated Domains Data

Field	Definition
C&C Host	A list of domains the destination IP addresses in the external server events resolved to.
Last Seen	The date and time of the most recent external server hit.

Signatures is a list of the threat indicators associated with the IP address.

Table 56: ETA Server Signature Data

Field	Definition
Name	The name or type of detected malware.
Category	Description of the malware and way in which it might have compromised a resource or resources.
Date	The date the malware was seen.

Certificates is a list of certificates associated with the external server. Click **View Certificate** and **Download Certificate**

Table 57: ETA Server Certificate Data

Field	Definition
Subject	Specifies the IP address of the external server
Issuer	Specifies the authority that issued the certificate.
SHA1	SHA1 hash of the server certificate.
Date/Time Seen	The date and time when the SHA1 file was last updated.

RELATED DOCUMENTATION

Encrypted Traffic Insights Overview and Benefits | 154

PART 5

Configure Juniper ATP Cloud Features

CHAPTER 17

Allowlists and Blocklists

IN THIS CHAPTER

Allowlist and Blocklist Overview

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

Benefits of Allowlists and Blocklists

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

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

1. Custom allowlist
2. Custom blocklist

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

Allowlists supported types are listed in Table 58 on page 164.

Table 58: Allowlists Supported Types

Type	Information
Anti-malware	IP address, URL, file hash, e-mail sender, and AI-PTP
SecIntel	C&C IP address and domain
ETI	IP address and hostname
DNS	Domains
Reverse Shell	Destination IP addresses and domains

NOTE: Domain refers to a fully qualified domain name (FQDN).

Blocklists supported types are listed in Table 59 on page 164.

Table 59: Blocklists Supported Types

Type	Information
Anti-malware	IP address, URL, file hash, and e-mail sender
SecIntel	C&C IP address and domain

NOTE:

- For the file hash type, the files are downloaded to the client and sent to Juniper ATP Cloud to be checked against the anti-malware blocklists, regardless of whether you set the advanced anti-malware (AAMW) policy to permit or block.
- For IP and URL, The Web UI performs basic syntax checks to ensure your entries are valid.

- The cloud feed URL for allowlists and blocklists is set up automatically for you when you run the op script to configure your SRX Series Firewall. See "Download And Run the Juniper ATP Cloud Script" on page 26.

- A hash is a unique signature for a file generated by an algorithm. You can add custom allowlist and blocklist hashes for filtering, but they must be listed in a text file with each entry on a single line. You can only have one running file containing up to 15,000 file hashes. For upload details, see "Create Allowlists and Blocklists" on page 168. Note that Hash lists are slightly different than other list types in that they operate on the cloud side rather than the SRX Series Firewall side. This means the web portal is able to display hits on hash items.

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

Use the `show security dynamic-address instance advanced-anti-malware` CLI command to view the IP-based allowlists and blocklists on your SRX Series Firewall. There is no CLI command to show the domain-based or URL-based allowlists and blocklists.

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

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

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

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

Use the `show services security-intelligence category summary` CLI command to display summary for the specified SecIntel category.

Example show services security-intelligence category summary

```
user@host> show services security-intelligence category summary
...........
Category name     :Blacklist
  Status          :Enable
  Description     :Blacklist data
  Update interval :3600s
```

```
    TTL             :3456000s
    Feed name       :blacklist_domain
      logical-system:root-logical-system
      Vrf name      :junos-default-vrf
      Version       :20211013.4
      Objects number:0
      Create time   :2021-10-13 16:50:44 UTC
      Update time   :2024-12-05 17:08:29 UTC
      Update status :N/A
      Expired       :Yes
      Status        :Active
      Options       :N/A
    Feed name       :blacklist_ip
      logical-system:root-logical-system
      Vrf name      :junos-default-vrf
      Version       :N/A
      Objects number:0
      Create time   :2021-10-13 16:51:18 UTC
      Update time   :2024-12-05 17:08:29 UTC
      Update status :N/A
      Expired       :Yes
      Status        :Active
      Options       :N/A
 ............
 Category name     :Whitelist
   Status          :Enable
   Description     :Whitelist data
   Update interval :1800s
   TTL             :3456000s
   Feed name       :whitelist_ip
     logical-system:root-logical-system
     Vrf name      :junos-default-vrf
     Version       :N/A
     Objects number:0
     Create time   :2023-03-20 23:32:59 UTC
     Update time   :2024-12-05 17:10:17 UTC
     Update status :N/A
     Expired       :Yes
     Status        :Active
     Options       :N/A
```

Use the `show security dynamic-address instance default` CLI command to display the total number of default matching entries.

Example show security dynamic-address instance default

```
root@SRX-30-GW> show security dynamic-address instance default
No.     IP-start             IP-end                Feed
Address                       CountryCode
1       10.0.90.165           10.0.90.165           CC/2                              ID-
fffc0821                      --
2       10.0.128.88           10.0.128.88           CC/2                              ID-
fffc0821                      --
3       10.0.128.112          10.0.128.112          CC/2                              ID-
fffc0821                      --
4       10.0.128.209          10.0.128.209          CC/2                              ID-
fffc0821                      --
5       10.0.131.69           10.0.131.69           CC/2                              ID-
fffc0821                      --
6       10.0.132.55           10.0.132.55           CC/2                              ID-
fffc0821                      --
...........
```

Use the `show security dynamic-address category-name Blacklist` CLI command to view the list of locations such as IP addresses and URLs that you do not trust.

Example show security dynamic-address category-name Blacklist

```
root@SRX-30-GW> show security dynamic-address category-name Blacklist
No.     IP-start             IP-end               Feed
Address                       CountryCode
1       10.1.1.1              10.1.1.1               Blacklist/2
ID-80004420                      --
2       10.2.2.100            10.2.2.100             Blacklist/2
ID-80004420                      --

Instance default Total number of matching entries: 2
```

Use the `show security dynamic-address category-name Whitelist` CLI command to view the list of locations such as IP addresses and URLs that you trust.

Example show security dynamic-address category-name Whitelist

```
root@SRX-30-GW> show security dynamic-address category-name Whitelist
No.     IP-start             IP-end               Feed
```

```
Address                        CountryCode
1       10.10.10.10          10.10.10.11          Whitelist/1
ID-80004010                        --

Instance default Total number of matching entries: 1
```

RELATED DOCUMENTATION

Create Allowlists and Blocklists | 168

Create Allowlists and Blocklists

IN THIS SECTION

Access these pages from **Configure** > **Allowlists** or **Configure** > **Blocklists**.

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

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

Before You Begin

- Read the "Allowlist and Blocklist Overview" on page 163 topic.
- Decide on the type of item you intend to define:
  - URL
  - IP
  - File Hash

- E-mail sender
- AI-PTP
- C&C
- ETI
- DNS

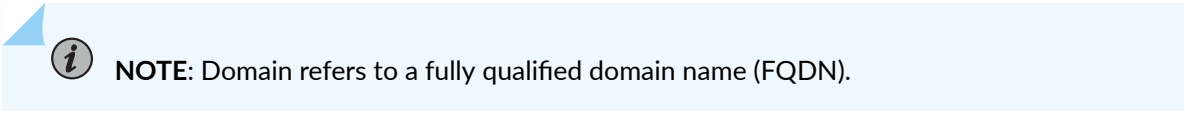
- Review current list entries to ensure the item you are adding does not exist.
- If you are uploading hash files, the files must be in a text file (TXT) with each hash on its own single line.

Create Allowlists

1. Select **Configure** > **Allowlists**.
2. Select one of the types mentioned in Allowlists Supported Types on page 169.

   Table 60: Allowlists Supported Types

Type	Information
Anti-malware	IP address, URL, file hash, e-mail sender, and AI-PTP
SecIntel	C&C IP address and domain
ETI	IP address and hostname
DNS	Domains
Reverse Shell	Destination IP addresses and domains



NOTE: Domain refers to a fully qualified domain name (FQDN).

3. Enter the required information.
4. Click **OK**.

Create Blocklists

1. Select **Configure** > **Blocklists**.
2. Select one of the types mentioned in Blocklists Supported Types on page 170.

   Table 61: Blocklists Supported Types

Type	Information
Anti-malware	IP address, URL, file hash, and e-mail sender
SecIntel	C&C IP address and domain

3. Enter the required information.
4. Click **OK**.

See the following tables for the data required by each type.

IP

When you create an IP list item, you must select the Type of list as **IP**. You must enter the required information. See the following table.

Table 62: IP Configuration

Setting	Guideline
IP	Enter the IPv4 or IPv6 IP address. For example: 1.2.3.4 or 0:0:0:0:0:ffff:0102:0304. CIDR notation and IP address ranges are also accepted. Any of the following IPv4 formats are valid: 1.2.3.4, 1.2.3.4/30, or 1.2.3.4-1.2.3.6. Any of the following IPv6 formats are valid: 1111::1, 1111::1-1111::9, or 1111:1::0/64. **NOTE**: Address ranges: No more than a block of /16 IPv4 addresses and /48 IPv6 addresses are accepted. For example, 10.0.0.0-10.0.255.255 is valid, but 10.0.0.0-10.1.0.0 is not. Bitmasks: The maximum amount of IP addresses covered by bitmask in a subnet record for IPv4 is 16 and for IPv6 is 48. For example, 10.0.0.0/15 and 1234::/47 are not valid.

NOTE: To edit an allowlist or blocklist IP entry, select the check box next to the entry you want to edit, click the pencil icon and click **OK**.

URL

When you create a URL list item, you must choose the Type of list: **URL**. Enter the required information. See the following table.

Table 63: URL Configuration

Setting	Guideline
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 allowlist or blocklist URL entry, select the check box next to the entry you want to edit, click the pencil icon and click **OK**.

File Hash

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

Table 64: Hash File Upload and Edit Configuration

Field	Guideline
You can add custom allowlist and blocklist hashes for filtering, but these hashes must be listed in a TXT with each entry on a single line. You can only have one running hash file containing up to 15,000 file hashes. This file contains the “current” list, but you can add to it, edit it, and delete it at any time.	

Table 64: Hash File Upload and Edit Configuration *(Continued)*

Field	Guideline
SHA-256 Hash Item	To add to hash entries, you can upload several TXT files and these files will automatically combine into one file. See all, merge, delete and replace options below. **Download**—Click this button to download the TXT if you want to view or edit it. You can select any of the following options from the **Select Hash File Items Upload Option** drop-down list: • **Replace current list**—Use this option when you want to change the existing list, but do not want to delete it entirely. Download the existing file, edit it, and then upload it again. • **Merge with current list**—Use this option when you upload a new TXT and want it to combine with the existing TXT file. The hashes in both files combine to form one text file containing all hashes. • **Delete from current list**—Use this option when you want to delete only a portion of the current list. In this case, you would create a TXT file containing only the hashes you want to remove from the current list. Upload the file using this option and only the hashes in the uploaded file are deleted from the current active list. **Delete All** or **Delete Selected**—Sometimes it is more efficient to delete the current list rather than downloading it and editing it. Click this button to delete the current selected list or all lists that have been added and accumulated here.
Source	This field indicates either Allowlist or Blocklist.
Date Added	The month, date, year, and time when the hash file was last uploaded or edited.

Email Sender

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

Table 65: Email Sender Configuration

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

If an email matches the blocklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment. The email is blocked and a replacement email is sent. If an email matches the allowlist, that email is allowed through without any scanning. See "Quarantined Emails Overview" on page 138.

It is worth noting that attackers can easily fake the “From” email address of an email, making blocklists a less effective way to stop malicious emails.

AI-PTP

Juniper Networks' AI-Predictive Threat Prevention is an advanced malware detection and prevention solution designed to safeguard your network against threats arising from users accessing corporate resources from various locations and browsing the Internet to many destinations. Powered by AI and ML, this intelligent security solution enhances the ability to predict and identify genuine threats more swiftly, allowing human experts to concentrate on strategic security initiatives.

For more information about AI-Predictive Threat Prevention (AI-PTP), see AI-Predictive Threat Prevention Overview.

You can use the AI-PTP tab to add, replace, merge, or delete AI-PTP signatures in the allowlists. You can add the file signatures that are identified as false positives to the allowlists. This process excludes the specified signatures from malware inspection performed by the SRX Series Firewalls.

To add or edit a list of signatures:

1. Select **Configure** > **Allowlists** > **ANTI-MALWARE** > **AI-PTP**.

   The AI-PTP Signature page is displayed.

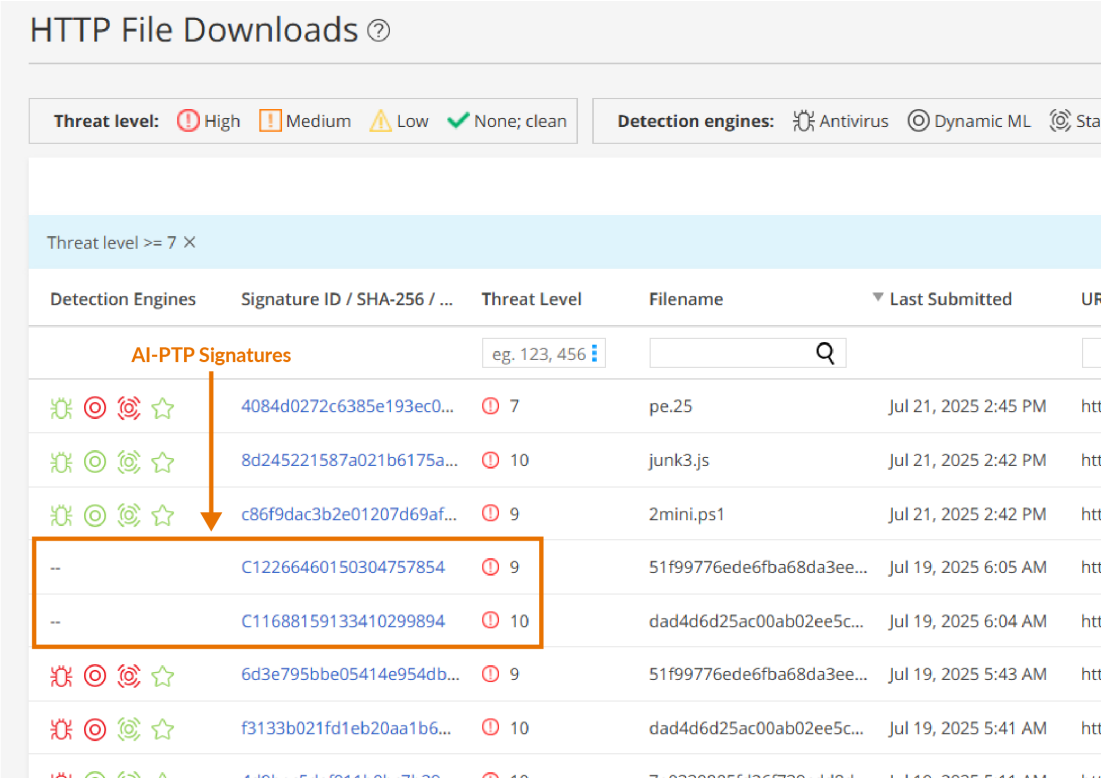
2. Select any of the following options from the **Signature File Upload Option** drop-down list:

   - **Replace current list**—Upload a text file (TXT) containing a list of file signatures or modify the existing list without deleting it. Download, edit, and re-upload the file. You can upload multiple TXT files that will automatically combine into one file.

     You can obtain AI-PTP signatures from the following sources:

     - HTTP File Downloads—Navigate to **Monitor** > **Files** > **HTTP File Downloads**

Figure 34: AI-PTP Signatures



- Email Attachments—Navigate to **Monitor** > **Files** > **Email Attachments**
- SMB File Downloads—Navigate to **Monitor** > **Files** > **SMB File Downloads**
- Syslogs on SRX Series Firewalls

- **Merge with current list**—Combine a new TXT with the existing file, creating a single file with all signatures.
- **Delete from current list**—Remove specific signatures. Create a TXT with the signatures to be removed, upload it, and only those signatures will be deleted.

The Upload Hash List window is displayed.

3. Browse your computer and select the TXT file.
4. Click **OK**.

The AI-PTP signatures are added to the allowlists.

Table 66 on page 176 describes the AI-PTP Signature fields.

Table 66: AI-PTP Signature Fields

Field	Description
Signature	Number of file signatures added to the allowlists
Date Added	Date and time when the file signatures list was last uploaded or edited.

5. Click **Download** to download the TXT if you want to view or edit it.

6. Click **Delete All** to delete all lists that have been added to the allowlists.

To view the list of advanced-anti-malware (AAMW) signatures added to the allowlists on SRX Series Firewalls, use the CLI command `show services advanced-anti-malware signature-exempt-list`.

```
show services advance-anti-malware signature-exempt-list
Advanced-anti-malware Signature Exempt List:
  J1994069136041805794
  C5381964424818232941
  J12111449344962437113
  C4660909146742838820
Total exempt signatures: 4
```

To view the list of anti-virus signatures added to the allowlists on SRX Series Firewalls, use the CLI command `show services anti-virus signature-exempt-list`.

```
Anti-virus Signature Exempt List:
  C1994069136041805794
  J5381964424818232941
  J12111449344962437113
  J4660909146742838820
Total exempt signatures: 4
```

To clear the file signature allowlists on the SRX Series Firewalls, use CLI command `clear services anti-virus signature-exempt-list`.

You can also run the following CLI commands on your SRX Series Firewalls to add, delete, export, and import file signatures:

- `request services anti-virus signature-exempt-list add <signature-id>`—add file signature IDs on your SRX Series Firewall. For example, `request services anti-virus signature-exempt-list add J4660909146742838820`.
- `request services anti-virus signature-exempt-list delete <signature-id>`—delete file signature IDs on your SRX Series Firewall. For example, `request services anti-virus signature-exempt-list delete J4660909146742838820`.
- `request services anti-virus signature-exempt-list import <txt-file-with-signature-ids>`—import TXT file that contains signature IDs on your SRX Series Firewall. For example, `request services anti-virus signature-exempt-list import /var/tmp/av-exempt-list.txt`.
- `request services anti-virus signature-exempt-list export <txt-file-with-signature-ids>`—export TXT file that contain signature IDs from your SRX Series Firewall. For example, `request services anti-virus signature-exempt-list export /var/tmp/av-exempt-list.txt`.

C&C Server

When you allowlist a C&C server, the SRX Series Firewalls receive the IP or hostname. The firewalls then exclude it from any SecIntel blocklists or C&C feeds, including Juniper's global threat feed and third-party feeds. The server will also now be listed under the C&C allowlist management page.

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

NOTE: You can also manage allowlist and blocklist entries using the Threat Intelligence API. When adding entries to the allowlist/blocklist data, these entries will be available in the Threat Intelligence API under the following feed names: "whitelist_domain" or "whitelist_ip", and "blacklist_domain" or "blacklist_ip." See the Juniper ATP Cloud Threat Intelligence Open API Setup Guide for details on using the API to manage any custom feeds.

Table 67: C&C Configuration

Field	Guideline
Type	Select IP to enter the IP address of a C&C server that you want to add to the allowlist. Select Domain to allowlist an entire domain on the C&C server list.

Table 67: C&C Configuration *(Continued)*

Field	Guideline
IP or Domain	For IP, enter an IPv4 or IPv6 address. An IP can be IP address, IP range or IP subnet. For domain, use the following syntax: juniper.net. Wildcards are not supported.
Description	Enter a description that indicates why an item has been added to the list.

You can also allowlist C&C servers directly from the C&C Monitoring page details view. See "Command And Control Servers: More Information" on page 95.

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

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

Encrypted Traffic Insights (ETI)

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

Table 68: Encrypted Traffic Configuration

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

Domain Name System (DNS)

You can specify the domains that you want to allowlist from DNS filtering. Use this tab to add, modify, or delete the allowlists for DNS filtering.

Table 69: Domains Configuration

Field	Guideline
URL	Enter the URL for domain that you want to allowlist.
Comments	Enter a description that indicates why the domain has been added to the list.

Reverse Shell

You can specify the IP addresses or domains that you want to allowlist from reverse shell detection. Use this tab to add, modify, or delete the allowlists for reverse shell detection.

Table 70: Reverse Shell Configuration

Field	Guideline
IP	Enter the IP address for the allowlist.
URL	Enter the URL for domain that you want to allowlist.

NOTE: Juniper ATP Cloud periodically polls for new and updated content and automatically downloads it to your SRX Series Firewall. You don't need to manually push your allowlist or blocklist files.

RELATED DOCUMENTATION

Allowlist and Blocklist Overview | 163

SecIntel Feeds Overview and Benefits | 202

CHAPTER 18

Email Scanning: Juniper ATP Cloud

IN THIS CHAPTER

Emails Overview

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

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

Benefits of Emails

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

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

For SMTP

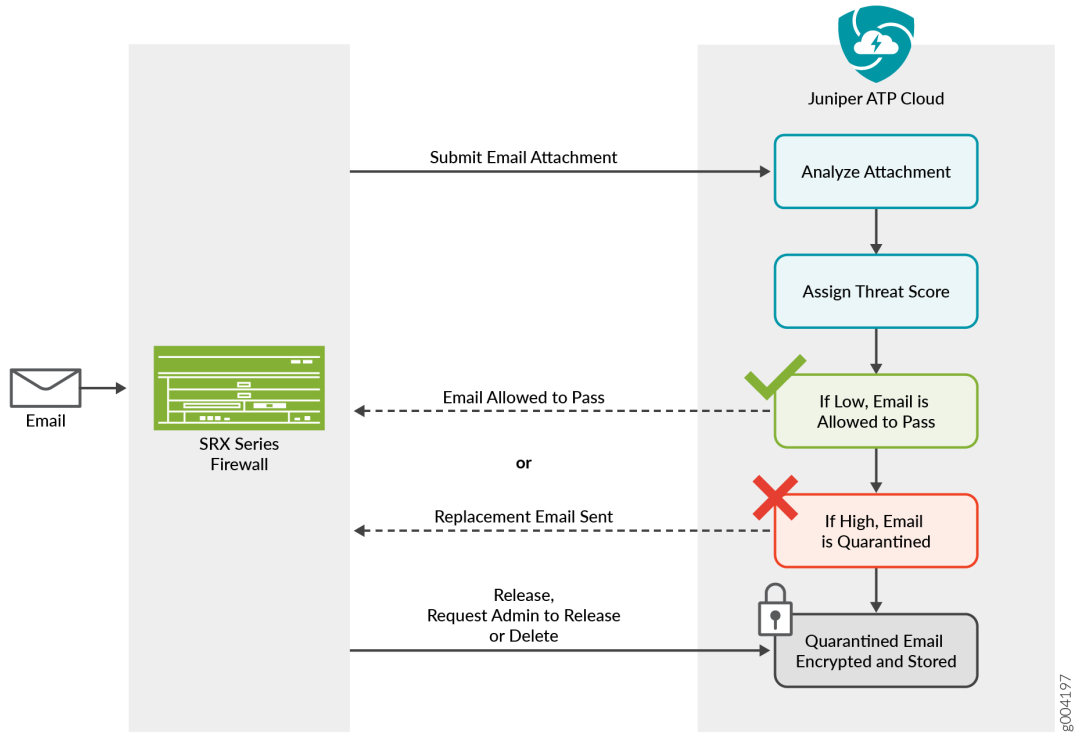
- Quarantine Malicious Messages—If you select to quarantine emails with attachments found to be malicious, those emails are stored in the cloud in an encrypted form and a replacement email is sent to the intended recipient. That replacement email informs the recipient of the quarantined message and provides a link to the Juniper ATP Cloud 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. Optionally, you can choose to send a notification to the end user about the permitted message.

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 35: Emails Overview



Quarantine Release

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

If you configure Juniper ATP Cloud to have the recipient send a request to the administrator to release the email, the recipient previews the email in the Juniper ATP Cloud 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.)

Blocklist and Allowlist

Emails are checked against administrator-configured blocklists and allowlists using information such as Envelope From (MAIL FROM), Envelope To (RCPT TO), Body Sender, Body Receiver. If an email matches the allowlist, that email is allowed through without any scanning. If an email matches the blocklist, it is considered to be malicious and is handled the same way as an email with a malicious attachment.

RELATED DOCUMENTATION

- Emails: Configure SMTP | 182
- Create Allowlists and Blocklists | 168
- Quarantined Emails Overview | 138

Emails: Configure SMTP

Access this page from **Configure** > **Emails** > **SMTP**.

- Read the "Emails Overview" on page 180 topic.
- Decide how malicious emails are handled: quarantined, delivered with headers, or permitted.

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

Table 71: 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 about the quarantining. Both the email and the attachment are stored in the cloud in an encrypted format.

Table 71: Configure Quarantine Malicious Messages *(Continued)*

Setting	Guideline
Release option	• Recipients can release email—This option provides recipients with a link to the Juniper ATP Cloud 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. **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. • Recipients can request administrator to release email—This option also provides recipients with a link to the Juniper ATP Cloud 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. **NOTE**: When a quarantined email is released, it is allowed to pass through the SRX Series Firewall with a header message that prevents it from being quarantined. 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.
Email Notifications for End Users	
Learn More Link URL	If you have a corporate website 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 about their quarantined email. For this custom message, enter a subject indicating a suspicious email sent to the recipient has been quarantined, such as "Malware Detected."
Custom Message	Enter information to help email recipients understand what they should do next.

Table 71: Configure Quarantine Malicious Messages *(Continued)*

Setting	Guideline
Custom Link Text	Enter custom text for the Juniper ATP Cloud quarantine portal link where recipients can preview quarantined emails and take action on these emails.
Buttons	• 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 72: Configure Deliver with Warning Headers

Setting	Guideline
Action to take	Deliver with warning headers—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	• 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 precede headers with information for the recipient, such as "Possible Spam."
Buttons	• Click **Reset** to clear all fields without saving. • Click **OK** if you are satisfied with the configuration.

Table 73: Permit

Setting	Guideline
Action to take	Permit—You can select to permit the message. Optionally, you can choose to send a notification to the end user about the permitted message containing an unknown malware.
Notify end users	Enable this option to configure the notification domain and send custom notifications to the notification domain users and administrators. If this field is disabled, then the notification is sent only to the administrators.
Protected Domains	(Optional) Enter comma-separated list of domain names. By default, malware notification is sent to configured administrators and end users of all domains. When you specify the protected domains, the malware notification will only be sent to the users in the specified domains.
Subject	When an email is permitted and **Notify end user** is enabled, the recipient receives a custom message about their permitted email containing an unknown malware. For this custom message, enter a subject indicating a suspicious email sent to the recipient has been permitted, such as "Malware Notification."
Custom Message	(Optional) Enter information to help email recipients understand what they should do next. Default predefined message will be sent if left blank.
Email Notifications for Administrators	
Subject	When an email is permitted, the administrator receives a custom message about the permitted email. For this custom message, enter a subject indicating a suspicious email sent to the recipient has been permitted, such as "Malware Notification."
Custom Message	Enter information to help email recipients understand what they should do next.

Table 73: Permit *(Continued)*

Setting	Guideline
Buttons	• Click **Preview** to view the custom message that will be sent to a recipient when an email is permitted. 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 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

Emails Overview | 180

Quarantined Emails Overview | 138

Configure the SMTP Emails Policy on the SRX Series Firewall

Emails: Configure IMAP

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

- Read the "Emails Overview" on page 180 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** > **Emails** > **IMAP**.

2. Based on your selections, configuration options will vary. See the tables below.

Table 74: Configure Block Malicious Messages

Setting	Guideline
Action to take	• Permit download of malicious attachments—Allow email attachments, either from all IMAP servers or specific IMAP servers, through to their destination. **NOTE**: In Permit mode, blocklists and allowlists are not checked. Emails from blocklisted addresses are not sent to the cloud for scanning. They are allowed through to the client. • Block download of malicious attachments—Block email attachments, either from all IMAP servers or specific IMAP servers, from reaching their destination. **NOTE**: In Block mode, black and allowlists are checked. Emails from blocklisted addresses are blocked. Emails from allowlisted 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. **NOTE**: If a blocked email has multiple recipients, any individual recipient can request to release the email and all recipients will receive it. When you select to block email attachments, in place of the original email, intended recipients receive a custom email you configure with information about the block action. Both the email and the attachment are stored in the cloud in an encrypted format.

Table 74: Configure Block Malicious Messages *(Continued)*

Setting	Guideline
IMAP Server	• 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. When you add IMAP servers to the list, it is sent to the SRX Series Firewall to filter emails sent to Juniper ATP Cloud for scanning. For emails that are sent for scanning, if the returned score is above the set policy threshold on the SRX Series Firewall, then the email is blocked.
IMAP Servers	Select the **Specific IMAP Server** option above and click the **+** sign to add IMAP server hostnames to the list. **NOTE**: You must use the IMAP server hostname and not the IP address.
Email Notifications for End Users	
URL to learn more about Policy	If you have a corporate website 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 about their blocked email. For this custom message, enter a subject indicating a suspicious email sent to the recipient has been blocked, such as "Malware Detected."
Custom Message	Enter information to help email recipients understand what they should do next.
Custom Link Text	Enter custom text for the Juniper ATP Cloud quarantine portal link where recipients can preview blocked emails and take action on these emails.

Table 74: Configure Block Malicious Messages *(Continued)*

Setting	Guideline
Buttons	• 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 clear 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

Blocked Attachments Overview | **140**

Emails Overview | **180**

Configure the IMAP Emails Policy on the SRX Series Firewall

CHAPTER 19

File Inspection Profiles

IN THIS CHAPTER

File Inspection Profiles Overview

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

Juniper ATP Cloud 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 to scan. Then enter the profile names on eligible SRX Series Firewalls to apply them.

Benefits of File Inspection Profiles

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

Table 75: File Category Contents

Category	Description	File Types
Archive	Archive files	.zip, .rar, .tar, .gzip
Configuration	Configuration files	.inf, .ini, .lnk, .reg, .plist

Table 75: File Category Contents *(Continued)*

Category	Description	File Types
Document	All document types except PDFs	.chm, .doc, .docx, .dotx, .hta, .html, .pot, .ppa, .pps, .ppt, .pptsm, .pptx, .ps, .rtf, .txt, .xlsx, .xml, .xsl, .xsl
Executable	Executable binaries	.bin, .com, .dat, .exe, .msi, .msm, .mst
ELF	Executable and Linkable Format (ELF) is a standard file format for executable files, object code, and libraries.	
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
Mobile	Mobile formats	.apk, .ipa
OS package	OS-specific update applications	.deb, .dmg

Table 75: File Category Contents *(Continued)*

Category	Description	File Types
PDF	PDF, e-mail, and MBOX files	.email, .mbox, .pdf, .pdfa
Rich Application	Installable Internet Applications such as Adobe Flash, JavaFX, Microsoft Silverlight	.swf, .xap, .xbap
Script	Scripting files	.bat, .js, .pl, .ps1, .py, .sh, .tcl, .vbs

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

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

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

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

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

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

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

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

```
Advanced Anti-malware inspection profile:
Profile Name:default_profile version: 1443769434 disabled_file_types: { ...
```

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

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

RELATED DOCUMENTATION

- Create File Inspection Profiles | 193
- Enroll an SRX Series Firewall Using Juniper ATP Cloud Web Portal | 51
- Remove an SRX Series Firewall from Juniper ATP Cloud | 58
- Juniper Licensing User Guide

Create 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 190 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 standard or advanced model of Juniper ATP Cloud, you are limited to only the executable file category. For more licensing information, see Software Licenses for ATP Cloud.

To create a device profile:

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

Table 76: Device Profile Settings

Setting	Guideline
Name	Enter a unique name for the profile. This name 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	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: **Do not scan** – This file type is not processed for scanning and is always allowed through. **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. **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.

NOTE: You can create up to 32 profiles.

NOTE: Juniper ATP Cloud periodically polls for new and updated content and automatically downloads it to your SRX Series Firewall. You don't need to manually push your profile.

RELATED DOCUMENTATION

SecIntel Feeds Overview and Benefits | 202

File Inspection Profiles Overview | 190

Juniper Advanced Threat Prevention Cloud License Types

CHAPTER 20

Adaptive Threat Profiling

IN THIS CHAPTER

Adaptive Threat Profiling Overview and Configuration

IN THIS SECTION

Overview

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

This feature allows you to configure security or IDP policies that, when matched, inject the following into a threat feed:

- Source IP address
- Destination IP address
- Source identity
- Destination identity

Other devices can use this threat feed as a dynamic-address-group (DAG). While this feature is focused on tracking and mitigating threat actors within a network, you can also use it for non-threat related activities, such as device classification.

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

NOTE: This feature requires a SecIntel License (Premium model) to function. Additional detection capabilities might require AppID, IDP, and Enhanced Web Filtering (EWF) licenses to be added to your device if not already present. For information about other licensed features, see Software Licenses for ATP Cloud.

Benefits of adaptive threat profiling

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

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

Table 77: Adaptive Threat Profiling

Field	Guideline
Feed Name	Name of the adaptive threat profiling feed.
Items	Number of entries in the feed.
Feed Type	Content type of the feed. The following options are supported: • IP • USER_ID

Table 77: Adaptive Threat Profiling *(Continued)*

Field	Guideline
Added to Infected Hosts	Displays whether the feed content (for example, source or destination IP address) is added to the Infected host feed. • True—The feed content is added to the Infected host feed. • False—The feed content is not added to the Infected host feed. **NOTE**: Currently you can add only IP address feed type to the Infected host feed.
Time to Live (days)	Defines how long an entry will "live" inside the feed. Once the TTL is reached, the entry is removed automatically.

NOTE:

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

You can perform the following tasks from this page:

- Add a new feed—See "Create an Adaptive Threat Profiling Feed" on page 199.
- Modify a feed—Select a feed and click the edit icon (pencil). The Edit *<feed-name>* page appears, displaying the same fields that were presented when you create a feed. Modify the fields as needed. Click **OK** to save your changes.

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

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

- Excluded Items—Lists all the IP addresses or User IDs that are excluded from the feed. To remove an IP address or User ID for the excluded items list, select the IP address or User ID and click the Delete icon.

  To manually exclude an IP address or User ID from the feed:

  1. Click the plus (+) icon in the Excluded Items tab.

     The Add to Excluded List page appears.

  2. Enter the IP address or User ID that you want to exclude from the feed.

  3. Click **OK**.

     The IP address or User ID is listed in the Excluded items page.

Configure Adaptive Threat Profiling

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

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

1. Check the URL for the feed server.

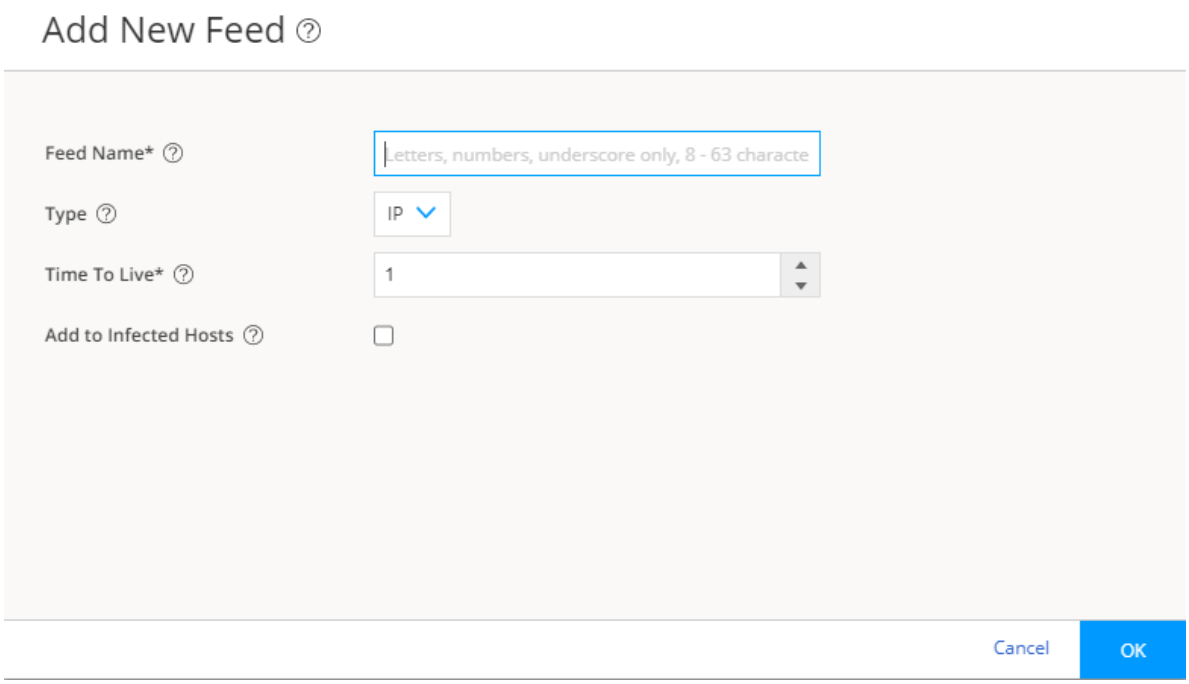
   Your output should look similar to the following:

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

   NOTE: If the URL is not present in the configuration, try re-enrolling the device in Juniper ATP Cloud. See "Enroll an SRX Series Firewall Using Juniper ATP Cloud Web Portal" on page 51.

2. Create an adaptive threat profiling feed in Juniper ATP Cloud. Log into Juniper ATP Cloud UI, select **Configure** > **Adaptive Threat Profiling**. The Adaptive Threat Profiling page appears as shown in Figure 36 on page 199. In this example, we will use the feed name **High_Risk_Users** with a time-to-live (TTL) of seven days.

Figure 36: Add New Feed



3. Click **OK** to save changes. For more information, see "Create an Adaptive Threat Profiling Feed" on page 199.

4. Ensure that the feed has been downloaded by your SRX Series Firewall. This is done automatically at regular intervals but can take a few seconds.

   A manual download of the SecIntel database can speed up this process, if necessary.

   See Juniper Advanced Threat Prevention Cloud Administration Guide for more information.

RELATED DOCUMENTATION

Create an Adaptive Threat Profiling Feed | 199

Create an Adaptive Threat Profiling Feed

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

Review the "Adaptive Threat Profiling Overview and Configuration" on page 195 topic.

To add a new adaptive threat profiling feed:

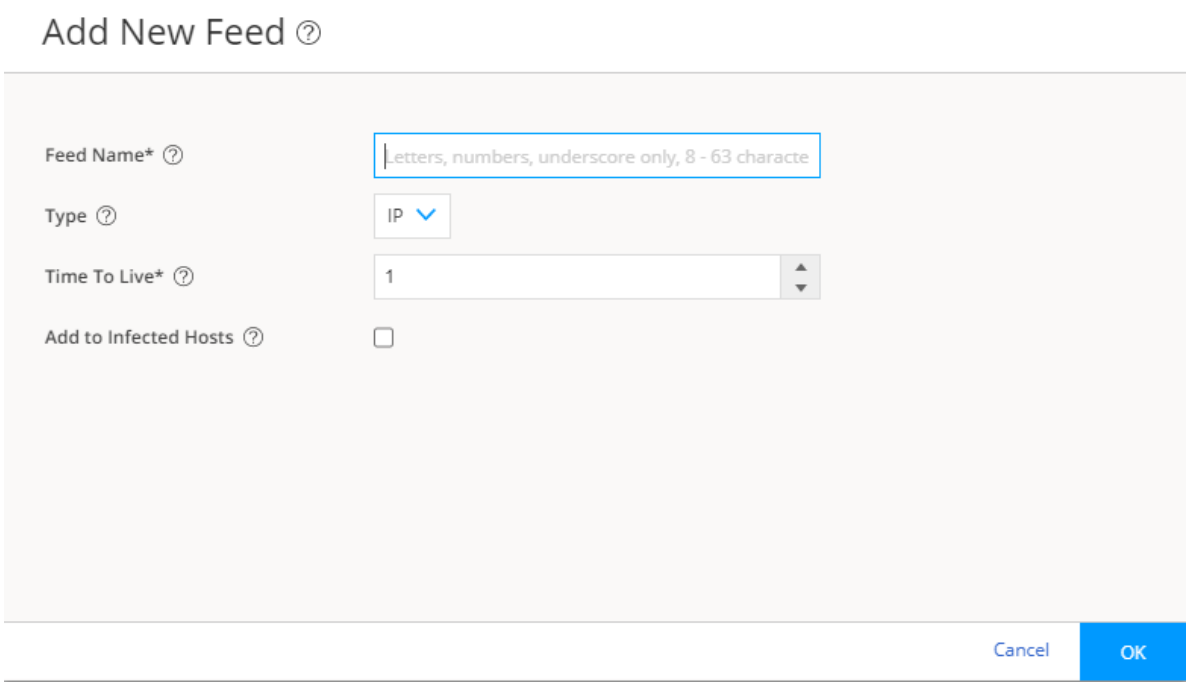
1. Select **Configure** > **Adaptive Threat Profiling**.

   The Adaptive Threat Profiling page appears.

2. Click the plus sign (+).

   The Add New Feed page appears as shown in Figure 37 on page 200.

Figure 37: Add New Feed Settings



3. Complete the configuration according to the guidelines provided in the Table 78 on page 200.
4. Click **OK** to save the changes.

Table 78: Add New Feed Settings

Setting	Guideline
Feed Name	Enter a unique name for the threat feed. The feed name must begin with an alpha-numeric character and can include letters, numbers, and underscores; no spaces are allowed. The length is 8–63 characters.

Table 78: Add New Feed Settings *(Continued)*

Setting	Guideline
Type	Select the content type of the feed. The following options are available: • IP • User ID
Data Source	The data source (User Policy) of the feed is auto-selected. You cannot modify this field.
Time to Live	Enter the number of days for the required feed entry to be active. After the feed entry crosses the time to live (TTL) value, the feed entry is automatically removed. The available range is 1–365 days.
Add to Infected Hosts	(Optional) Enable this setting to add the contents (for example, source or destination IP address) from this feed to the Infected host feed. **NOTE**: Currently, you can only add IP addresses to Infected host feed.

NOTE:

- You can create a maximum of 64 feeds.
- You can add all 64 feeds to infected host feeds.
- After you create a feed, the same feed will be available for configuration on the Junos CLI.

RELATED DOCUMENTATION

Adaptive Threat Profiling Overview and Configuration | 195

CHAPTER 21

Feeds Configuration

IN THIS CHAPTER

SecIntel Feeds Overview and Benefits

SecIntel collects carefully curated and verified threat intelligence from:

- Juniper ATP Cloud
- Juniper Threat Labs
- Dynamic Address Group (DAG)
- Industry-leading threat feeds

SecIntel delivers this intelligence to MX Series routers, SRX Series Firewalls, and NFX Series Network Services Platform to block Command and Control (C&C) communications at line rate. SecIntel delivers real-time threat intelligence by enabling automatic and responsive traffic filtering.

SecIntel integrates with EX Series Switches and QFX Series Switches and enables these switches to subscribe to SecIntel's infected host feed. This integration enables you to block compromised hosts at the switch port. You can now extend SecIntel throughout your entire network and increase the number of security enforcement points.

Benefits of SecIntel Feeds

You can view all the default feeds available with your current license.

Using this page, you can enable the following feeds for integration with Juniper ATP Cloud.

- Juniper threat feeds
- Third party threat feeds—IP threat feeds and URL threat feeds.

- Dynamic address group feeds—Juniper DAG feeds and Third-party DAG feeds.

> **NOTE**: The expiry of the SecIntel feeds depends upon the time-to-live (TTL) value, which is different for each feed.

> **NOTE**: The total number of C&C feeds are 32, out of which four feeds are reserved for cc_ip, cc_url, cc_ipv6, and cc_cert_sha1. So, you can enable up to 28 feeds to the C&C category, which includes C&C custom feeds and third-party feeds. This limit 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** > **Threat Sources** with a threat level of 10.
- On enrolled SRX Series Firewalls, you can configure policies with the permit or block action for each feed. Note that C&C and Infected Host feeds require an enabled SecIntel policy on the SRX Series Firewall in order to work.
- External feeds are updated once every 24 hours.

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

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

To enable the available feeds, do the following:

1. Navigate to **Configure** > **Feeds Configuration** > **SecIntel Feeds**.
2. For each feed, select the toggle button to enable the feed. Refer to the guidelines in Table 79 on page 204.

   > **NOTE**: The Infected Host feed is enabled for all license tiers. For licensing information about all other Juniper SecIntel feeds, see Software Licenses for ATP Cloud.

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

Table 79: SecIntel Feeds

Field	Guidelines
Juniper Threat Feeds	
Command and Control	Displays whether the C&C feed is enabled or not.
Malicious Domains	Displays whether the DNS feed is enabled or not.
Infected Host Feed	Displays whether the infected host feed is enabled or not.
Third Party Threat Feeds	
IP Threat Feeds	
Block List	Click the toggle button to enable block list feeds as third party feeds. Predefined cloud feed name— cc_ip_blocklist.
Threatfox IP	Click the toggle button to enable Threatfox feeds as third party feeds. Predefined cloud feed name— cc_ip_threatfox.
Feodo Tracker	Click the toggle button to enable Feodo feeds as third party feeds. Predefined cloud feed name— cc_ip_feodotracker.
DShield	Click the toggle button to enable DShield feeds as third party feeds. Predefined cloud feed name— cc_ip_dhield.
Tor	Click the toggle button to enable tor feeds as third party feeds. Predefined cloud feed name— cc_ip_tor.
URL Threat Feeds	

Table 79: SecIntel Feeds *(Continued)*

Field	Guidelines
Threatfox URL	Click the toggle button to enable Threatfox feed as third party feeds. ThreatFox is a free platform from abuse.ch with the goal of sharing indicators of compromise (IoC) associated with malware with the infosec community, antivirus vendors and threat intelligence providers. The IOC can be an IP address, domain name, or URL. Predefined cloud feed name— cc_url_threatfox.
URLhaus URL Threat Feed	Click the toggle button to enable URLhaus feed as third party feeds. URLhaus is a threat intelligence feed that shares malicious URLs that are used for malware distribution. Predefined cloud feed name— cc_url_urlhaus.
Open Phish	Click the toggle button to enable OpenPhish feed as third party feeds. OpenPhish is a fully automated self-contained platform for phishing intelligence. It identifies phishing sites and performs intelligence analysis in real time without human intervention and without using any external resources, such as blocklists. For malware inspection, SecIntel will analyze traffic using URLs in this feed. Predefined cloud feed name— cc_url_openphish.
Domain Threat Feeds	
Threatfox Domains	Click the toggle button to enable Threatfox feed as third party feeds. Predefined cloud feed name— cc_domain_threatfox.
Dynamic Address Group Feeds	
Juniper DAG Feeds	
GeoIP Feed	Displays whether the GeoIP feed is enabled or not. GeoIP feed 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.

Table 79: SecIntel Feeds *(Continued)*

Field	Guidelines
Third Party DAG Feeds	
office365	Click the toggle button to enable office365 IP filter feed as a third party feed. The office365 IP filter feed is an up-to-date list of published IP addresses for Office 365 service endpoints which you can use in security policies. This feed works differently from others on this page and requires certain configuration parameters, including a predefined cloud feed name of “ipfilter_office365”. See more instructions at the bottom of this page, including usage of the `set security dynamic-address` command for using this feed. Predefined cloud feed name— ipfilter_office365
facebook	Click the toggle button to enable feeds from Facebook. Predefined cloud feed name— ipfilter_facebook
google	Click the toggle button to enable feeds from Google. Predefined cloud feed name— ipfilter_google
atlassian	Click the toggle button to enable feeds from Atlassian. Predefined cloud feed name— ipfilter_atlassian
zscaler	Click the toggle button to enable feeds from Zscaler. Predefined cloud feed name— ipfilter_zscaler
zpa zscaler	Click the toggle button to enable feeds from Zscaler Private Access (ZPA). The ZPA service provides secure access to the applications and services within your organization. Pre-defined cloud feed name— ipfilter_zscaler_zpa
oracleoci	Click the toggle button to enable feeds from Oracle oci. Predefined cloud feed name— ipfilter_oracleoci

Table 79: SecIntel Feeds *(Continued)*

Field	Guidelines
cloudflare	Click the toggle button to enable feeds from Cloudflare. Predefined cloud feed name— ipfilter_cloudflare
zoom	Click the toggle button to enable feeds from Zoom. Predefined cloud feed name— ipfilter_zoom
microsoftazure	Click the toggle button to enable feeds from Microsoft Azure. Predefined cloud feed name— ipfilter_microsoftazure You can filter and view the DAG feeds from Azure regions and services that are relevant to you. To configure DAG filters for Azure feeds, click **Configure**, and follow the instructions in "Add and Manage DAG Filters" on page 211.
amazonaws	Click the toggle button to enable feeds from AWS. Pre-defined cloud feed name— ipfilter_amazonaws You can filter and view the DAG feeds from AWS regions and services that are relevant to you. To configure DAG filters for AWS feeds, click **Configure**, and follow the instructions in "Add and Manage DAG Filters" on page 211.
okta	Click the toggle button to enable feeds from Okta. Predefined cloud feed name— ipfilter_okta
paypal	Click the toggle button to enable feeds from Paypal. Predefined cloud feed name— ipfilter_paypal

NOTE:

- Starting in Junos OS Release 19.4R1, third party URL feeds are supported on Juniper ATP Cloud.

- Since Ransomware Tracker and Malware Domain list are deprecated, ransomware tracker and malware domain list IP feeds are not supported on Juniper ATP Cloud. If you had enabled this feed earlier, you might stop receiving these feeds.
- The update interval for a third party Internet service feed is one day.

3. Like other C&C and infected host feeds, enabled third party feeds require a SecIntel policy on the SRX Series Firewall in order to work. Example commands are provided here. See the Juniper Advanced Threat Prevention Cloud CLI Reference Guide for more information.

   On the SRX Series Firewall, configure a SecIntel Profile

```
set services security-intelligence profile secintel_profile category CC

set services security-intelligence profile secintel_profile rule secintel_rule match threat-level 10

set services security-intelligence profile secintel_profile rule secintel_rule match threat-level 9

set services security-intelligence profile secintel_profile rule secintel_rule then action block close

set services security-intelligence profile secintel_profile rule secintel_rule then log

set services security-intelligence profile secintel_profile default-rule then action permit

set services security-intelligence profile secintel_profile default-rule then log

set services security-intelligence profile ih_profile category Infected-Hosts

set services security-intelligence profile ih_profile rule ih_rule match threat-level 10

set services security-intelligence profile ih_profile rule ih_rule then action block close

set services security-intelligence profile ih_profile rule ih_rule then log

set services security-intelligence policy secintel_policy Infected-Hosts ih_profile

set services security-intelligence policy secintel_policy CC secintel_profile
```

4. The SecIntel policy must also be added to an SRX Series Firewall policy.

   On the SRX Series Firewall, configure a Security Policy. Enter the following commands to create a security policy on the SRX Series Firewall 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 about configuring the SRX Series with Juniper ATP Cloud using the available CLI commands, see the Juniper Advanced Threat Prevention Cloud CLI Reference Guide.

Using the office365 Feed

1. Enable the**Using the office365 Feed** check box in Juniper ATP Cloud to push Microsoft Office 365 services endpoint information (IP addresses) to the SRX Series Firewall. The office365 feed works differently from other feeds on this page and requires certain configuration parameters, including a pre-defined name of “ipfilter_office365”.

2. After you enable the check box, you must create a dynamic address object on the SRX Series Firewall that refers to the ipfilter_office365 feed as follows:

```
set security dynamic-address address-name office365 profile category IPFilter feed ipfilter_office365
```

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

A sample security policy is as follows:

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

Use the following command to verify the office365 feed has been pushed to the SRX Series Firewall. `Update Status` should display `Store succeeded`..

```
show services security-intelligence category summary
```

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

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

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

```
No.      IP-start             IP-end               Feed             Address
1        x.x.x.x         x.x.x.x         IPFilter/ipfilter_office365 office365
2        x.x.x.x         x.x.x.x         IPFilter/ipfilter_office365 office365
3        x.x.x.x        x.x.x.x        IPFilter/ipfilter_office365 office365
4        x.x.x.x        x.x.x.x         IPFilter/ipfilter_office365 office365
5        x.x.x.x         x.x.x.x         IPFilter/ipfilter_office365 office365
6        x.x.x.x        x.x.x.x          IPFilter/ipfilter_office365 office365
7        x.x.x.x         x.x.x.x         IPFilter/ipfilter_office365 office365
8        x.x.x.x         x.x.x.x          IPFilter/ipfilter_office365 office365
9        x.x.x.x         x.x.x.x          IPFilter/ipfilter_office365 office365
10       x.x.x.x         x.x.x.x          IPFilter/ipfilter_office365 office365
11       x.x.x.x        x.x.x.x        IPFilter/ipfilter_office365 office365
12       x.x.x.x         x.x.x.x         IPFilter/ipfilter_office365 office365
13       x.x.x.x        x.x.x.x        IPFilter/ipfilter_office365 office365
```

RELATED DOCUMENTATION

Hosts Overview | **75**

Host Details | **79**

Add and Manage DAG Filters | **211**

Juniper Threat Feeds Overview

SecIntel feeds include threat feeds provided by Juniper Networks, 3rd party threat feeds, or Dynamic Address Group (DAG) feeds. The SecIntel threat feeds provided by Juniper Networks is shown in Table 80 on page 211.

NOTE: The Infected Host feed is enabled by default for all license tiers. For licensing information about all other Juniper Threat feeds, see Software Licenses for ATP Cloud.

Table 80: Juniper Threat Feeds

Field	Guidelines
Command and Control Feed	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.
Malicious Domains (DNS)	List of domains that are known to be connected to malicious activity.
Infected Host Feed	Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or exhibit other symptoms.

RELATED DOCUMENTATION

SecIntel Feeds Overview and Benefits | 202

Add and Manage DAG Filters

IN THIS SECTION

Access the Dynamic Address Group (DAG) Filter page from the **Configure** > **Feeds Configuration** > **DAG Filter** menu.

Use a DAG filter to add feeds for the AWS and Azure regions and services that you select. You can configure a maximum of 10 DAG filters for AWS and Azure.

If you do not configure any DAG filter, generic feeds from all AWS and Azure regions and services are displayed. You must configure at least one DAG filter to avoid seeing these generic feeds.

Benefits

You can filter and view the feeds from specific AWS or Azure regions and services relevant to you.

Add DAG Filters

1. Select **Configure** > **Feeds Configuration** > **DAG Filter**.

   The DAG Filters page is displayed.

2. Select either AWS or the Azure tab.

3. Click the plus icon (+).

   The Add <*AWS or Azure*> DAG Filter window is displayed.

4. (Optional) In the **Description** field, enter a description for the DAG filter.

5. Select a region from the **Region** drop-down list.

   When you select a region, the Service drop-down list is available for Azure DAG filter.

6. Select a service from the **Service** drop-down list.

   When you select the region and service for AWS or Azure, the DAG filter name is automatically generated in the Name field. You cannot edit the DAG filter name.

   NOTE: The exact names for AWS and Azure regions and services are shown in the Name field for the DAG filter. This mapping is relevant only for the manifest file to ensure the DAG feed name is compatible with SRX Series Firewalls.

   Junos OS allows a maximum of 32 characters for the DAG filter name. If the feed name is longer than this limit, the cloud feeds manifest file will not display the feed name.

7. Click **OK**.

You can see the DAG feeds from the selected region and service in the DAG Filter page.

Table 81: DAG Filters Fields

Field	Description
Name	Auto-generated feed name based on selected region and service. The name includes the selected region and service. For example, if the name of the feed is ap-northeast-2_ROUTE53_RESOLVER, ap-northeast-2 is the region, and ROUTE53_RESOLVER is the service you selected for the feed.
Region	Selected AWS or Azure region
Feed Name	Feed name displayed in the manifest.xml file. For example: ipfilter_aws_ap-northeast-2_RT53, ipfilter_azure_APAC_Azrrcnfrstrc
Service	Selected AWS or Azure service
Last Changed	Date and time of the most recent feed update
Changed By	Email of the user who updated the feed
Description	Description of the AWS or Azure feed

8. Verify the feed name in the manifest.xml file. For example, if the feed name is ipfilter_aws_ap-northeast-2_RT53, it will appear as follows.

```
<feed data_ts="1753249858" logical_domain="root-logical-system" name="ipfilter_aws_ap-northeast-2_RT53" objects="25" options="" ttl="157680000" types="ip_addr ip_range ip_subnet ipv6_addr ipv6_range" update_interval="1800" version="20230707.1" vrf="junos-default-vrf">
<data>
```

9. Run the CLI command `set security dynamic-address address-name amazonaws profile category IPFilter feed <feed-name-in-manifest-file>` on SRX Series Firewalls to add AWS feeds,

```
set security dynamic-address address-name amazonaws profile category IPFilter feed
ipfilter_aws_ap-northeast-2_RT53
```

10. Run the CLI command `set security dynamic-address address-name microsoftazure profile category IPFilter feed <feed-name-in-manifest-file>` on SRX Series Firewalls to add Azure feeds.

```
set security dynamic-address address-name microsoftazure profile category IPFilter feed
ipfilter_azure_APAC_Azrrcnfrstrc
```

11. Run the CLI command `show security dynamic-address category-name IPFilter feed-name <feed name in manifest file>` on SRX Series Firewalls to view the added feeds.

```
show security dynamic-address category-name IPFilter feed-name ipfilter_aws_ap-
northeast-2_RT53
No.     IP-start             IP-end               Feed
Address                       CountryCode
1       10.34.89.64          10.34.89.127          IPFilter/ipfilter_aws_ap-
northeast-2_RT53 amazonaws               --
2       10.36.3.96           10.36.3.127           IPFilter/ipfilter_aws_ap-
northeast-2_RT53 amazonaws               --
3       10.36.3.160          10.36.3.175           IPFilter/ipfilter_aws_ap-
northeast-2_RT53 amazonaws               --
4       10.36.3.192          10.36.3.223           IPFilter/ipfilter_aws_ap-
northeast-2_RT53 amazonaws               --
5       10.36.3.224          10.36.3.255           IPFilter/ipfilter_aws_ap-
northeast-2_RT53 amazonaws               --
```

```
show security dynamic-address category-name IPFilter feed-name
ipfilter_azure_APAC_Azrrcnfrstrc
No.     IP-start             IP-end               Feed
Address                       CountryCode
1       10.145.72.0          10.145.72.7           IPFilter/
ipfilter_azure_APAC_Azrrcnfrstrc microsoftazure          --
2       10.145.72.8          10.145.72.9           IPFilter/
ipfilter_azure_APAC_Azrrcnfrstrc microsoftazure          --
3       10.190.132.42        10.190.132.43         IPFilter/
```

```
ipfilter_azure_APAC_Azrrcnfrstrc microsoftazure          --
4       10.190.132.184       10.190.132.191        IPFilter/
ipfilter_azure_APAC_Azrrcnfrstrc microsoftazure          --
5       10.200.250.192       10.200.250.193        IPFilter/
ipfilter_azure_APAC_Azrrcnfrstrc microsoftazure          --
6       10.240.144.50        10.240.144.51         IPFilter/
ipfilter_azure_APAC_Azrrcnfrstrc microsoftazure          --
7       10.240.144.80        10.240.144.87         IPFilter/
ipfilter_azure_APAC_Azrrcnfrstrc microsoftazure          --
8       10.243.24.48         10.243.24.55          IPFilter/
ipfilter_azure_APAC_Azrrcnfrstrc microsoftazure          --
9       10.243.24.56         10.243.24.57          IPFilter/
ipfilter_azure_APAC_Azrrcnfrstrc microsoftazure          --
```

Manage DAG Filter

- **Edit**—Select the DAG filter, and then click the pencil icon ( ).
- **Delete**—Select the DAG filter, and then click the trash can icon ( ).

RELATED DOCUMENTATION

SecIntel Feeds Overview and Benefits | 202

CHAPTER 22

Infected Hosts

IN THIS CHAPTER

Configuration for Infected Hosts

Threat Level Threshold for Blocking

Set the global threat level to block infected hosts. When a host is found to be compromised, it is assigned a threat level. Based on the global threat level you set here, 1-10 with 10 being the highest threat, compromised hosts with the set threat level and above are added to the infected hosts lists and can subsequently be blocked by policies configured on the SRX Series Firewall. See "Hosts Overview" on page 75 and Configure the SRX Series Firewall to Block Infected Hosts for more information.

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

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

Configure Threat Level Threshold for Blocking and Email Alerts

Benefits of the Global Infected Hosts Alerts

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

1. Select **Configure** > **Infected Hosts**.
2. (Advanced licenses only) Set the default threat level threshold.

3. Click the plus sign to create e-mail alerts, or click the pencil icon to edit existing ones. Configure the fields described in the table below.

4. Click **OK**.

Table 82: Email alerts for infected hosts fields

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

Automatically Expire Blocked Hosts

When a host is marked as infected and added to the infected hosts feed, it is blocked from the network by policies configured on the SRX Series Firewall. There are options for unblocking individual hosts on the **Host Details** page in the Juniper ATP Cloud Web Portal. See "Hosts Overview" on page 75 for information. If you want to unblock multiple host IP addresses based on time period and threat level, you would use the **Automatically Expire Blocked Hosts** feature on the **Infected Hosts** page in the Web Portal.

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

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

Configure Automatic Expiration of Infected Hosts

1. Select **Configure** > **Infected Hosts**.

2. (System Administrators and Operators only) Enable **Automatically Expire Blocked Hosts** and select one of the following:

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

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

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

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

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

3. For both **Expire all hosts** or **Expire a range of hosts**, you must also set expiration time and threat levels. Click the plus **+** sign to create an entry and set the following in the **Expiration Time** table.

Table 83: Expiration time fields

Setting	Guideline
Set the Minimum Threat Level	Click the table entry under **Minimum Threat Level** to access a pulldown menu. Select a minimum threat level (1-10). The level you select is included in the minimum setting.
Set the Maximum Threat Level	Click the table entry under **Maximum Threat Level** to access a pulldown menu. Select a maximum threat level (1-10). The level you select is included in the maximum setting.
Set the Hours to Unblock	Click the table entry under **Hours to Unblock**. You can select Never, 6, 12, 18, or 24 hours. After the set amount of hours, the infected label expires and the hosts are no longer blocked.
For example, if you set the minimum at 6 and the maximum at 8 with hours to unblock as 24, the following would occur. All infected hosts with a threat level of 6 and above and 8 and below would expire after 24 hours. **NOTE**: You can create multiple entries in this table, setting different expiration times for different threat levels. Once unblock settings are entered in the table, you can use the table to change existing settings or to delete settings.	

4. Click **Save** to save your settings.

RELATED DOCUMENTATION

- Configure the SRX Series Firewall to Block Infected Hosts
- Hosts Overview | **75**
- Modify My Profile | **239**
- Create and Edit User Profiles | **241**

CHAPTER 23

Threat Intelligence Sharing

IN THIS CHAPTER

Configure Threat Intelligence Sharing

Using the TAXII service, Juniper ATP Cloud can contribute to STIX reports by sharing the threat intelligence it gathers from file scanning. Juniper ATP Cloud also uses threat information from STIX reports as well as other sources for threat prevention. See "HTTP File Download Details" on page 107 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. "Create Application Tokens" on page 243.

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

1. Select **Configure** > **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. "Create Application Tokens" on page 243.

Table 84: Additional Information

TAXII URLs and Services	Description
Discovery URL	Used by the TAXII client to discover available TAXII Services. The command to initiate a TAXII request is: `taxii-discovery` **NOTE**: For information about additional commands, see the TAXII documentation. Juniper ATP Cloud Discovery URLs are: US Region: https://taxii.sky.junipersecurity.net/services/discovery EU Region: https://taxii-eu.sky.junipersecurity.net/services/discovery APAC Region: https://taxii-apac.sky.junipersecurity.net/services/discovery Canada: https://taxii-canada.sky.junipersecurity.net/services/discovery
At this time, there are two services supported by Juniper ATP Cloud on the TAXII server.	
Collection Management	Used by the TAXII client to request information about available data collections. Juniper ATP Cloud Collection Management URLs are: US Region: https://taxii.sky.junipersecurity.net/services/collection-management EU Region: https://taxii-eu.sky.junipersecurity.net/services/collection-management APAC Region: https://taxii-apac.sky.junipersecurity.net/services/collection-management Canada: https://taxii-canada.sky.junipersecurity.net/services/collection-management

Table 84: Additional Information *(Continued)*

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

RELATED DOCUMENTATION

HTTP File Download Details | **107**

Create Application Tokens | **243**

CHAPTER 24

Misc Configurations

IN THIS CHAPTER

Configure Trusted Proxy Servers

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

NOTE: Support starting in Junos OS 17.4R1.

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

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

With this in mind, X-Forwarded-For (XFF) is a standard header added to packets by a proxy server that includes the real IP address of the client making the request. Therefore, if you add trusted proxy servers IP addresses to the list in Juniper ATP Cloud, by matching this list with the IP addresses in the HTTP header (X-Forwarded-For field) for requests sent from the SRX Series Firewalls, Juniper ATP Cloud 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** > **Misc 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 | 75

Compromised Hosts: More Information | 81

Organization Overview

IN THIS SECTION

Organizations and Tenant Systems

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

WARNING: Unlike physical devices, which automatically make submissions to the organization they are enrolled in, tenant system submissions are ignored until they are explicitly associated with an organization using the Organization Management page in the Juniper ATP Cloud Web UI. See "Organization Management" on page 226 for those instructions.

For example, if a managed security service provider (MSSP) partitions customers by organization and then associates all SRX Series tenant systems for an individual customer with their assigned organization, that MSSP can deliver targeted threat prevention policies to multiple customers while allowing administrators to easily switch between organizations for monitoring purposes.

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

For monitoring, each tenant system is included in log file events and different administrators can be given varying levels of access to each organization. The main organization to which other organizations are attached would then serve as a “super organization” that provides a global view of key statistics across all organizations. To configure monitoring access to an organization, log into the organization as a “system administrator” and add users with the role of “observer.” See "Create and Edit User Profiles" on page 241 for details.

Configuration Overview

Attach new organizations to the current organization (the organization you currently logged into) in Juniper ATP Cloud by navigating to **Configure** > **Misc Configuration** > **Organization Management**. You must enter a Username and Password for the organization in order to attach it.

All the devices and tenant systems on the Enrolled Device page appear in the Organization Management page where you can change their organization associations. See "Organization Management" on page 226 for details.

When you associate organizations with devices or change those associations, it changes the way threat management is delivered to those devices, which can affect anti-malware and SecIntel policies. Be sure all changes in organization/device associations are well-planned and that the consequences are intentional.

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

NOTE: You cannot create new organizations from the Organization Management page. To create an organization, log out of the Web UI. Access the login screen and click the **Create Organization** link on the bottom left of the login window.

SRX Series and Tenant System Enrollment

When an SRX Series Firewall is enrolled to Juniper ATP Cloud, any tenant systems configured on the device are also enrolled. The names of associated tenant systems appear in the **Host** name field after a colon on the Devices page in ATP Cloud. For example, when you run the enroll script on an SRX Series Firewall with the host name **SRX650**, that host name appears in the list of enrolled devices. If SRX650 has several tenant systems, you would have multiple host name entries starting with SRX650 followed by a colon with the name of the tenant system. For example, **SRX650:subdomain1**.

RELATED DOCUMENTATION

Organization Management | 226

Tenant Systems: Security-Intelligence and Anti-Malware Policies | 228

Organization Management

Attach new organizations to the current organization and change organization associations by navigating to **Configure** > **Misc Configuration** > **Organization Management**. You must enter a Username and Password for the organization to attach it.

Note the following:

- Your role must be “system administrator” on Juniper ATP Cloud to see the Organization Management page.
- You must explicitly associate an enrolled logical domain with an organization before Juniper ATP Cloud can receive submissions from that logical domain.
- Easily switch between organizations using the **Organization** field at the top right of the Web UI. Click inside the organization name field and a drop-down with all the organization names appears. Select a new organization to view configurations for that organization. Note that switching between organizations is not available for all Web UI pages, only applicable ones. For example, you cannot switch the organization view from the Organization Management page.
- Review the "Organization Overview" on page 224 topic.

- Have the correct name of the organization you are attaching and your credentials for that organization. You must enter the organization credentials when attaching new organizations.
- Organization management makes it easy to change organization/device associations, but when you remove a device's organization association and create a new one, the new organization begins receiving files and events for that device. The old organization no longer will. Be sure that is your intention before changing existing associations.
- Organization associations are restricted by region. You cannot attach an organization from one region to an organization in another region.

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

1. Navigate to **Configure** > **Misc Configuration** > **Organization Management**.
2. Click the **Attach Organization** button on the upper right side of the page.
3. In the window, enter the credentials for the organization you are adding. Enter the **Username**, organization **Password**, and the **Organization** name.
4. Click **OK**. The organization is added to your list of organizations and attached to Juniper ATP Cloud.

To associate organizations with SRX Series Firewalls or SRX Series Firewall logical domains, do the following:

1. Navigate to **Configure** > **Misc Configuration** > **Organization Management**.
2. Select a check box beside the organization name and click the **Manage Devices** button on the upper right side of the page.

   You can select only one check box at a time for managing devices. If you select more than one check box, the **Manage Devices** button becomes unavailable
3. In the window that appears, available devices are listed on the left side. Devices that are already associated with the organization are listed on the right side. Select a device check box, and use the right arrow to associate that device.

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

   Changes in associations take place immediately.

   NOTE: When you remove a device's organization association and create a new one, the new organization begins receiving files and events for that device. The old organization will no longer receive files and events.
4. Click **OK** to close the window.

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

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

RELATED DOCUMENTATION

Organization Overview | 224

Tenant Systems: Security-Intelligence and Anti-Malware Policies | 228

Tenant Systems: Security-Intelligence and Anti-Malware Policies

IN THIS SECTION

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

NOTE: For information about using tenant systems with SRX Series Firewalls, please see the Junos documentation.

Tenant System Support for SecIntel Feeds

Starting in Junos OS 18.4, you can configure SecIntel profiles for tenant systems.

Tenant systems enroll to ATP Cloud when the associated SRX Series Firewall is enrolled. All tenant systems with enabled anti-malware or SecIntel policies appear in the ATP Cloud “Enrolled Devices” page with other SRX Series Firewalls.

WARNING: Unlike physical devices, which automatically make submissions to the organization they are enrolled in, tenant system submissions are ignored until they are associated with an organization using the Organization Management page in the Juniper ATP Cloud Web UI. See "Organization Management" on page 226 for those instructions.

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

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

```
set logical-systems TSYS1 services security-intelligence profile secintel_profile category CC
set logical-systems TSYS1 services security-intelligence profile secintel_profile rule
secintel_rule match threat-level 10
set logical-systems TSYS1 services security-intelligence profile secintel_profile rule
secintel_rule match threat-level 9
set logical-systems TSYS1 services security-intelligence profile secintel_profile rule
secintel_rule then action block close
set logical-systems TSYS1 services security-intelligence profile secintel_profile rule
secintel_rule then log
set logical-systems TSYS1 services security-intelligence profile secintel_profile default-rule
then action permit
set logical-systems TSYS1 services security-intelligence profile secintel_profile default-rule
then log
set logical-systems TSYS1 services security-intelligence policy p1 CC secintel_profile
set logical-systems TSYS1 services security-intelligence profile pf1 category Infected-Hosts
set logical-systems TSYS1 services security-intelligence profile pf1 default-rule then action
block drop
set logical-systems TSYS1 services security-intelligence profile pf1 default-rule then log
set logical-systems TSYS1 services security-intelligence policy p1 Infected-Hosts pf1
```

Use the following commands to create a security policy on the SRX Series Firewall for the inspection profiles.

```
set logical-systems TSYS1 security policies from-zone trust to-zone untrust policy 1 match
source-address any
set logical-systems TSYS1 security policies from-zone trust to-zone untrust policy 1 match
destination-address any
set logical-systems TSYS1 security policies from-zone trust to-zone untrust policy 1 match
application any
set logical-systems TSYS1 security policies from-zone trust to-zone untrust policy 1 then permit
application-services ssl-proxy profile-name ssl-inspect-profile-dut
set logical-systems TSYS1 security policies from-zone trust to-zone untrust policy 1 then permit
application-services security-intelligence-policy p1
```

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

```
root@SRX> show security dynamic-address category-name Infected-Hosts logical-system TSYS1
No.      IP-start        IP-end          Feed             Address
1        10.1.32.131     10.1.32.131     Infected-Hosts/1 ID-2150001a
2        10.1.32.148     10.1.32.148     Infected-Hosts/1 ID-2150001a
3        10.1.32.183     10.1.32.183     Infected-Hosts/1 ID-2150001a
4        10.1.32.201     10.1.32.201     Infected-Hosts/1 ID-2150001a
```

Or use the following:

```
User1@SRX:TSYS1> show security dynamic-address category-name Infected-Hosts
No.      IP-start        IP-end          Feed             Address
1        10.1.32.131     10.1.32.131     Infected-Hosts/1 ID-2150001a
2        10.1.32.148     10.1.32.148     Infected-Hosts/1 ID-2150001a
3        10.1.32.183     10.1.32.183     Infected-Hosts/1 ID-2150001a
4        10.1.32.201     10.1.32.201     Infected-Hosts/1 ID-2150001a
```

Tenant System Support for AAMW

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

As stated previously, the tenant system used in this example (TSYS1) must be associated with the correct organization in ATP Cloud for the policy to get applied to the intended device. See "Organization Management" on page 226 for ATP Cloud Web UI configuration details.

```
set logical-systems TSYS1 services advanced-anti-malware policy LP1 http inspection-profile
ldom_profile
set logical-systems TSYS1 services advanced-anti-malware policy LP1 http action block
set logical-systems TSYS1 services advanced-anti-malware policy LP1 http notification log
set logical-systems TSYS1 services advanced-anti-malware policy LP1 smtp inspection-profile
default_profile
set logical-systems TSYS1 services advanced-anti-malware policy LP1 smtp notification log
set logical-systems TSYS1 services advanced-anti-malware policy LP1 imap inspection-profile
default_profile
set logical-systems TSYS1 services advanced-anti-malware policy LP1 imap notification log
set logical-systems TSYS1 services advanced-anti-malware policy LP1 verdict-threshold 3
```

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

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

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

Or use the following:

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

```
Advanced-anti-malware configuration:
 Policy Name: LP1
  Default-notification  : Log
```

```
Whitelist-notification: Log
Blacklist-notification: Log
Fallback options:
  Action: block
  Notification: No Log
Inspection-profile: ldom_profile
Applications: HTTP
Verdict-threshold: 3
Action: block
Notification: Log
```

Security Profile CLI

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

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

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

- aamw-policy

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

- secintel-policy

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

Use the following command to view the security profiles:

```
show system security-profile all-resource
```

NOTE: For more information about the `set system security-profile` command for logical systems, see the Junos documentation.

RELATED DOCUMENTATION

Organization Management | 226

Organization Overview | 224

Enable Logging

You can select the event types that you want to log for the devices in your organization. The Juniper ATP Cloud logs yields information such as malware name, action taken, infected host, source of an attack, and destination of an attack. The devices in your organization uses the even logs to generate system logs (syslogs).

To enable logging, do the following:

1. Select **Configure** > **Misc Configuration** > **Logging**.
2. Click the **Malware** toggle button to log malware in your organization.
3. Click the **Host Status** toggle button to log the host status in your organization.

NOTE: You can log the Malware or the Host Status event or both the event types.

RELATED DOCUMENTATION

Viewing Juniper Advanced Threat Prevention Cloud System Log Messages

Enable Mist Integration with Juniper ATP Cloud

You can integrate Mist with Juniper ATP Cloud to share threat alerts detected by Juniper SRX Series Firewalls and ATP Cloud with Mist customers. The threat alerts allow administrators to quickly assess security risks on wireless networks and take appropriate actions, such as quarantine or enforce security policies.

The threat alerts shared by Juniper ATP Cloud with Mist includes malware downloads from websites, attempts to access malicious e-mail attachments, C&C hits (including Encrypted Traffic Insights C&C hits), and host status changes. The host status change includes mitigation events taken by the customer, such as resolving an event as Fixed, Ignored, or False Positive, on ATP Cloud Customer Portal.

Juniper ATP Cloud supports multiple Mist deployments that are connected to a single region. You can select the Mist to which you want to stream the security events.

Table 85 on page 234 lists the Sample Mist cloud certificates that are used while deploying multiple Mist. The Mist cloud certificate is securely shared with the Mist customers for their current and future deployments.

Table 85: Target Mist Cloud Details

Region	Target Mist Cloud	Mist ID
ATP Cloud US	manage.mist.com	us-west-1
	manage.gc1.mist.com	us-west2-a
	manage.ac2.mist.com	us-east-1
ATP Cloud EU	manage.eu.mist.com	eu-central-1

Benefits of integrating Mist with Juniper ATP Cloud:

- Adds another layer of security to the robust mechanisms already in place within the Mist WLAN platform.
- Leverages artificial intelligence (AI) for tighter security, lower operational costs and optimized user experience.
- Quickly identifies devices on the network that are infected with malware and takes appropriate actions.
- Allows to track client hosts better as Mist supplies client MAC addresses to Juniper ATP Cloud.

> **NOTE**: MAC address is available with Mist integration even if Policy Enforcer is not used.

Before you integrate Mist with ATP Cloud, you must enroll SRX Series Firewalls in both Juniper ATP Cloud organization and Mist sites.

- For information about enrolling SRX Series Firewalls in Juniper ATP Cloud organization, see "Enroll an SRX Series Firewall Using Juniper ATP Cloud Web Portal" on page 51.
- For information about enrolling SRX Series Firewalls in Mist sites, see Cloud-Ready SRX Series Firewalls with Mist.

To enable Juniper ATP Cloud in the Mist site:

1. In the Juniper Mist menu, select **Organization** > **Site Configuration**.

   The Sites page appears.

2. Click the site in which you want to enable Juniper ATP Cloud.

   The site information page appears.

3. Scroll down the page and select the **Enabled** option in the Juniper ATP section.

   Juniper ATP Cloud is now enabled in the Mist site.

4. Select the check box **Send IP-MAC Mapping to Juniper ATP** to receive Host IP and MAC Address.

To enable Mist integration in Juniper ATP Cloud portal:

1. Select **Configure** > **Misc Configuration** > **Mist**.
   The Enable Mist page appears.
2. Click the **Enable Mist** toggle button.
3. Select the target Mist cloud to stream your security events.
   Threat alerts are automatically streamed from Juniper ATP Cloud to your Mist.

RELATED DOCUMENTATION

Configuration for Infected Hosts | 216

Configure Webhook

Access the Audit Log Web Hook page from the **Configure** > **Misc Configuration** > **Webhook** menu.

A webhook is an automated message or real-time notification that your application receives from another application that triggers an event. It communicates data about the occurrence of an event in one system to another system. This communication of data happens over the web through a webhook URL.

You can use an audit log webhook to send Juniper ATP Cloud audit log notifications to a remote server. You can enable the webhook and configure the remote server URL to receive the audit log notifications in a chat application that can process JavaScript Object Notation (JSON) responses.

Before you begin:

- Configure your chat application to receive the audit log notifications. See Create Incoming Webhooks page for instructions to create a webhook.

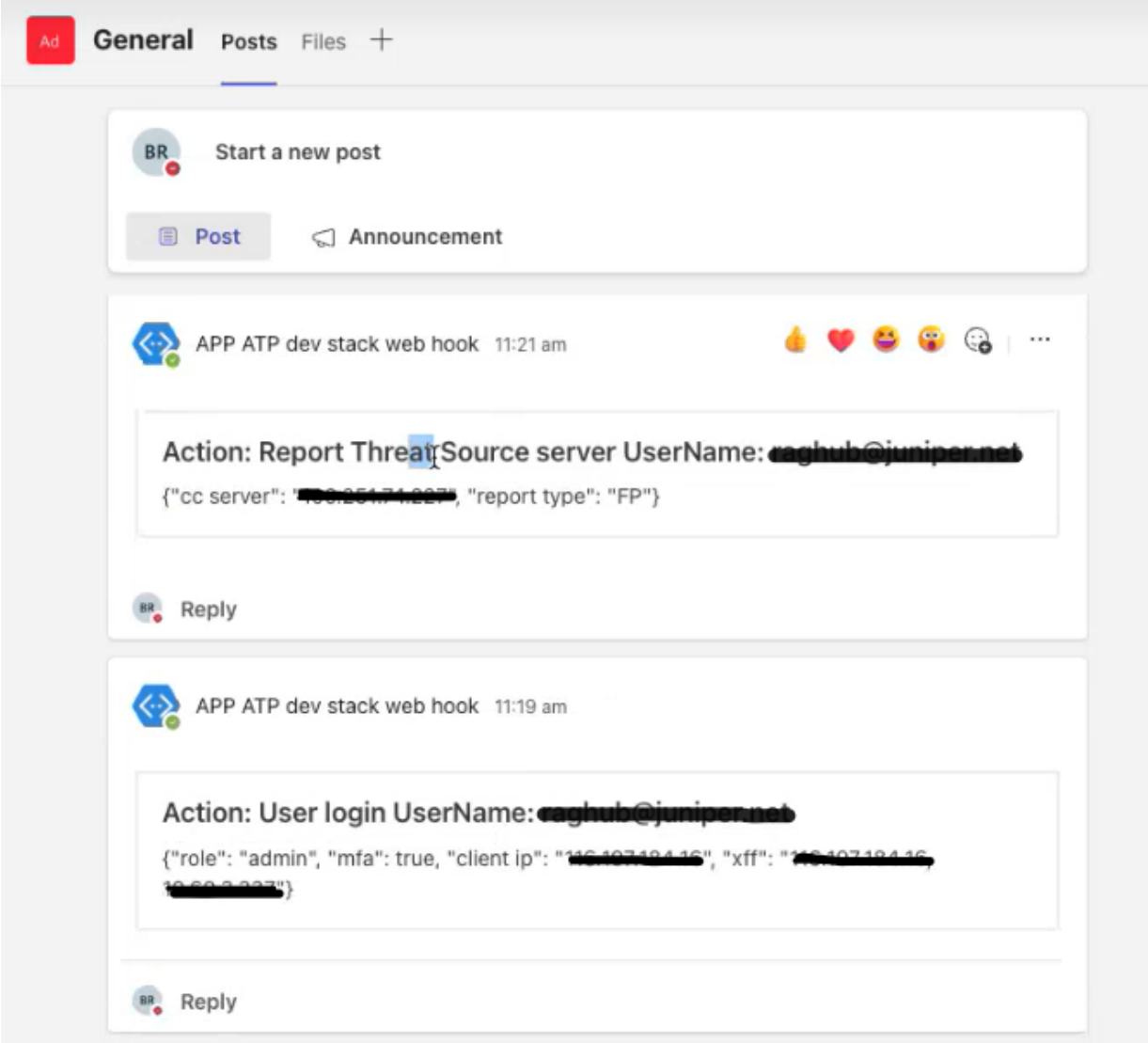
To enable and configure the webhook, do the following:

1. Select **Configure** > **Misc Configuration** > **Webhook**.
   The Audit Log Webhook page appears.

2. Select **Enable Webhook** toggle button to enable the Audit Log Webhook.
3. Copy and paste the URL from Create Incoming Webhooks page in the **Webhook URL** field.
4. Click **Save**.

Once configured, you will receive the audit log notifications in your chat application as shown in Figure 38 on page 236.

Figure 38: Audit Log Notifications in Teams



RELATED DOCUMENTATION

View Audit Logs | 268

PART 6

Administration

CHAPTER 25

Juniper ATP Cloud Administration

IN THIS CHAPTER

Modify My Profile

An administrator profile is created for you when you register for a Juniper ATP Cloud 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 Juniper ATP Cloud portal. It does not grant access to any SRX Series Firewall.

To update your administrator profile, do the following:

1. Select **Administration**.

   The My Profile landing page appears.
2. Edit the fields described in the table below.
3. Click **OK** to save your changes or click Reset to discard the changes.

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

Table 86: My Profile Fields

Setting	Guideline
First Name	Enter a string beginning with an alphanumeric character.
Last Name	Enter a string beginning with an alphanumeric character.
E-mail	Enter a valid e-mail address.
Password	Enter a unique string at least 8 characters long. Include both uppercase and lowercase letters, at least one number, and at least one special character (~!@#$%^&*()_-+={}[]|:;<>,./?); no spaces are allowed, and you cannot use the same sequence of characters that are in your username. Note that your username for Juniper ATP Cloud is your e-mail address.
Role Assignment	Change the role assignment: System administrator, Operator, or Observer
MFA Method	If multi-factor authentication is enabled, this field displays the verification method, SMS or Email. If this user is locked out for too many verification code requests, click the link to **Reset mobile number**. This removes the lock, allowing the user to step through the Verification Identity screen again. Note that there is no way to remove a lockout if the MFA method is Email.

RELATED DOCUMENTATION

Create and Edit User Profiles | 241

Reset Password | 46

Create and Edit User Profiles

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

- Review the "Modify My Profile" on page 239 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 administrator accounts:

1. Select **Administration** > **Users**.
2. Enter the information described in the table below.
3. Click **OK**.

Table 87: 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 Address	Enter a valid e-mail address.
Role Assignment	You can assign different roles to users to determine their level of access to configurations. When you create a user, select their role from the pulldown. Available roles are: • System Administrator—A system administrator has full write access to the Juniper ATP Cloud web portal and can edit all configuration information. Only a system administrator can create and edit user accounts. • Operator—An operator has write access to the Juniper ATP Cloud web portal and can edit all configuration information with the exception of user accounts. • Observer—An observer has read-access only to the Juniper ATP Cloud web portal with the exception of user accounts.

RELATED DOCUMENTATION

Modify My Profile | 239

Set Password

Use this page to set the password for Juniper ATP Cloud once a new user profile is created.

To set a new password:

The user will receive an email to their registered email address with a link to set the password.

1. Click the **Set Password** link to generate the password.

   You will be redirected to the Juniper ATP Cloud dashboard login page. The organization and email address of the user will be autopopulated.

   NOTE: The Set Password link is valid for only 24 hours.

2. In the **Password** field, enter your new password.

   The password must contain a minimum of 8 characters and must include at least one uppercase letter, one lowercase letter, one special character, and one number. No spaces are allowed. You cannot use the same sequence of characters that are in your username.

3. In the **Re-enter Password** field, enter your new password again.
4. Click **Continue**.

   The password is now reset. You should receive an email confirming the set password action.

   You can now login to Juniper ATP Cloud Web UI with the new password.

You can contact your system administrator to send the set password link again to the user's account in the following scenarios:

- Set password Link is no longer valid.
- Expired link
- Password is already set.

Application Tokens Overview

Use the Application Token page to view or add application tokens that allow Security Director or Open API users to securely access Juniper ATP Cloud APIs over HTTPS. Using the available buttons, you can mark tokens as active or inactive.

When a token is used, you can view the IP address of the user and the date of last usage by clicking the token name. Then you can block or unblock IP addresses that are trying to use individual tokens. An application token is marked inactive if it has not been used for 30 days. Once inactive, all access using the token is blocked until it is activated again. If an application token has not been used for 90 days, it is automatically deleted and cannot be recovered again.

Benefits of Application Tokens

- Limits the applications that can use Juniper ATP Cloud APIs and Juniper ATP Cloud threat information to only those that are authorized. For example, you can limit who has access to your shared threat information by creating an application token for TAXII. See "Configure Threat Intelligence Sharing" on page 220.
- Allows you to easily activate or deactivate a token from one central location

RELATED DOCUMENTATION

Create Application Tokens | 243

Create Application Tokens

To access this page, click **Administration** > **Application Tokens** > **Application Tokens**. You can generate application tokens from the App Tokens page.

- Review the "Application Tokens Overview" on page 242 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 88 on page 244 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 88: Application Token Settings

Field	Description
Name	Enter a unique name for this token. This name 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 is deactivated.

When you click an application token name, you can view the IP addresses of devices that have used the token and the time the token was utilized. To block and IP address or unblock it:

1. Select the check box beside the IP address.
2. Click the **Block** button. Use the **Unblock** button to reinstate access to the IP address.

RELATED DOCUMENTATION

Application Tokens Overview | 242

Command And Control Servers: More Information | 95

Multifactor Authentication Overview

Multifactor Authentication (MFA) requires a user to pass at least two different types of authentication before gaining access to a requested page. Juniper ATP Cloud lets you configure MFA (over SMS or Email) for administrators who are logging into the Juniper ATP Cloud Web UI or resetting their passwords. This setting is optional when enabled, applies globally to all administrators in an organization.

The benefits of MFA are:

- Improves security by minimizing the chances of unauthorized access to resources.
- Adds authentication layers with the ability to randomize login credentials and mitigate danger when user passwords are compromised.
- Allows systems to verify the identity of the user by contacting that user directly, thereby alerting the user to unauthorized access if the user did not initiate the login request.

When you enable MFA, you select to send a verification code by text or email when administrators attempt to login to Juniper ATP Cloud. The first time administrators try to login, they are prompted to enter their mobile number. Once that information is entered, they can receive a verification code. Once the code is entered and verified, the user can login the Juniper ATP Cloud Web UI.

RELATED DOCUMENTATION

Configure Multifactor Authentication for Administrators | 245

Configure Multifactor Authentication for Administrators

IN THIS SECTION

Enable Multifactor Authentication

When you enable multifactor authentication (MFA) for an organization, it is turned on for all administrators in an organization. You must be a System Administrator to enable MFA.

To enable and configure MFA settings, navigate to **Administration** > **Multifactor Authentication**.

1. Use the slider to enable MFA.
2. Select an authentication method. In this method, a verification code will be sent to the administrator, either **SMS** or **Email**.

   If you select Email, the configuration is finished, and you can click **Save**. ATP Cloud will use the email address already entered for each user. If you select SMS, continue to the next step.

   NOTE: A user is locked out of ATP Cloud for 1 hour if 4 verification codes have been sent without any being used (verified) to login to ATP Cloud.

   NOTE: When you change the authentication method, if any users have been locked out due to too many verification code requests, those users are all automatically unlocked. All counters that track the number of verification codes that have been sent are reset to zero when the authentication method is changed.
3. Select an **Authentication Interval**. The options are:
   - Every time user logs in—User must enter a verification code for every log in.
   - Every day—Multi-factor authentication is required every 24 hours. After going through the MFA process once, only username and password are required to log in until 24 hours have passed.
   - Every week—Every week—Multi-factor authentication is required every 7 days. After going through the MFA process once, only username and password are required to log in until 7 days have passed.
   - Month— MFA is required every 30 days. After going through the MFA process once, only username and password are required to log in until 30 days have passed.

   NOTE: The user can select a check box on the Verify Identity screen to remember the code for the period of time selected above. If the user does not click the check box, she will have to go through the verification process again no matter what authentication interval is configured.
4. Click **Save**.

Verification Codes for MFA: SMS

When SMS is set as the authentication method, the first time an administrator attempts to log in to the Juniper ATP Cloud Web UI (enters a username and password), a Verify Identity screen appears. Administrators must enter the following information in the Verify Identity screen:

- Select the country where the mobile number was issued.
- Enter their mobile phone number (numbers only, no dashes or other characters)
- Click the **Send Code** button. A verification code is sent to the mobile device.
- Once the code is received by text or email, enter the 8 digit code in the Verification Code field.
- Click **Verify**.

Lockout Conditions:If an administrator does not receive the code, she can click the Send Code button again. Note the following security precautions in place for resending code requests: ATP Cloud will wait 60 seconds after sending a code before it will send another code once a request is made. Once a user has requested a verification code 4 times without logging in to ATP Cloud, she is permanently locked out. In this case, the user must contact an administrator to remove the lock.

Verification Codes for MFA: Email

When Email is set as the authentication method, the first time an administrator attempts to log in to the Juniper ATP Cloud Web UI (by entering a username and password), a Verify Identity screen appears. You must enter the following information:

- Enter the 8 digit verification code contained in the email.
- Click **Verify**.

If you did not receive the code, check your spam folder. If the code is not in spam folder, you can click the **Resend Code** button. Note the following security rules for resending code requests. ATP Cloud will wait 60 seconds after sending a code before it will send another code once a request is made. If you request a verification code four times without logging in to ATP Cloud, you will be locked out for an hour. You can then request a new code after one hour.

NOTE: When Email is the MFA method, the one hour lockout cannot be cleared. The user must wait the full hour before requesting another verification code.

Unlock a User

An SMS lockout can be removed by a system administrator who is logged into Juniper ATP Cloud.

To remove the lockout,

1. Navigate to **Administration** > **Users** and locate the locked out user.
2. Select the check box to edit the user.
3. On the User Edit screen is MFA Method and Mobile Number. Click the link to **Reset mobile number**. This removes the lock, allowing the user to step through the Verification Identity screen again, and the code request counter is reset to zero.

RELATED DOCUMENTATION

Multifactor Authentication Overview | 245

Set Up Single Sign-on with SAML 2.0 Identity Provider

IN THIS SECTION

Single sign-on (SSO) is an authentication method that allows you to securely log in to multiple applications and websites with a single set of login credentials.

Security Assertion Markup Language (SAML) is a framework for authentication and authorization between a service provider and an identity provider (IdP). Here, authentication is exchanged using digitally signed XML documents. The service provider agrees to trust the IdP to authenticate users. In return, the IdP generates an authentication assertion indicating that a user is authenticated.

Benefits

- With SAML authentication, you can easily integrate Juniper ATP Cloud with your corporate IdP to provide SSO. If you are authenticated to your IdP, you are automatically authenticated to Juniper ATP Cloud. You need not remember separate passwords or type in credentials every time you access the Juniper ATP Cloud portal.

- We support SAML protocol only for service provider-initiated SSO. Juniper ATP Cloud is compatible with SAML 2.0 web SSO profile as a service provider.

Step1: Configure SSO Settings in IdP

Example: Configure SSO with Okta as IdP

This section provides step-by-step instructions to configure SSO with Okta as IdP:

NOTE:

- The information provided in this section is based on the current SSO with SAML implementation by Okta and is subject to change. For more detailed information, see Okta Documentation.
- You must already have an account with Okta.
- You must log in as administrator to perform the following operations.

1. Log in to Okta portal.
2. Navigate to Applications and click **Applications > Create App Integration**.
3. In the Sign in method section, select **SAML 2.0** and click **Next**.
4. Enter the General settings for your application, such application name, application logo, and application visibility. Click **Next**.
5. Configure the SAML Setting. For guidelines, see Table 89 on page 250.
6. Click **Next**.
7. Choose whether you are a customer or a partner. Click **Finish**.
   Your application is now added to Okta. Click the **Sign on** tab. The Okta IdP metadata file is available for download. You can use this metadata file to dynamically import Okta IdP SSO settings to Juniper ATP Cloud.
8. Navigate to **Directory > Groups > Add Group** and add groups. Create separate groups for each roles. For example, role_administrator, role_operator, role_observer.
   The group names are important. Note down the group names as it will be used for user role mapping in Juniper ATP Cloud Portal. See Table 92 on page 255
   .
9. Click on a group name and add users and applications to the group.

10. Click **Manage People** and select the users from the list. The user is now added from **Not Members** list to the **Members** list.

11. Click **Save**. The user is now assigned to the group.

Table 89: SSO SAML Settings for Okta

Field	Description
General Settings	
Single sign on URL	The location where the SAML assertion is sent with a HTTP POST. This is often referred to as the SAML Assertion Consumer Service (ACS) URL for your application. Example: *https://canada.sky.junipersecurity.net/portal/sso/acs*
Audience URI (SP Entity ID)	The application-defined unique identifier that is the intended audience of the SAML assertion. This is Juniper ATP Cloud's SP Entity ID (a globally unique identifier). Example: *https://canada.sky.junipersecurity.net*
Default Relay State	(Optional) Identifies a specific application resource in an IdP-initiated Single Sign-On scenario. In most instances this field is blank. Juniper ATP Cloud does not support IdP-initiated SSO. We recommend you leave this field blank.
Name ID format	Identifies the SAML processing rules and constraints for the assertion's subject statement. Select the name ID format from the list. Use the default value of 'Unspecified' unless the application explicitly requires a specific format. This field is not used in the Juniper ATP Cloud Web portal, hence retain the default value.

Table 89: SSO SAML Settings for Okta *(Continued)*

Field	Description
Application username	Determines the default value for a user's application username. The application username is used for the assertion's subject statement. Select the application username from the list. This field is not used in the Juniper ATP Cloud, hence retain the default value.
Advanced Settings	
Response	Determines whether the SAML authentication response message is digitally signed by IDP or not. A digital signature is required to ensure absolute privacy of the information exchanged by your IdP. You must set this field to **Signed**.
Assertion Signature	Determines whether the SAML assertion is digitally signed or not. A digital signature is required to ensure that only your IDP generated the assertion. You must set this field to **Signed**.
Signature Algorithm	Determines the signing algorithm used to digitally sign the SAML assertion and response. Okta provides RSA-SHA256 signature algorithm.
Digest Algorithm	Determines the digest algorithm used to digitally sign the SAML assertion and response. Okta provides SHA256 digest algorithm.

Table 89: SSO SAML Settings for Okta *(Continued)*

Field	Description
Assertion Encryption	Determines whether the SAML assertion is encrypted or not. Encryption ensures that nobody but the sender and receiver can understand the assertion. You must set this field to encrypted only if you plan to enable **Encrypt SAML response** on the Juniper ATP Cloud ATP SSO settings.
Enable Single Logout	Enable SAML Single Logout. This field is not used in the Juniper ATP Cloud, hence retain the default value.
Assertion Inline Hook	This field is disabled. This field is not used in the Juniper ATP Cloud, hence retain the default value.
Authentication context class	Identifies the SAML authentication context class for the assertion's authentication statement This field is not used in the Juniper ATP Cloud, hence retain the default value.
Honor Force Authentication	Prompt user to re-authenticate, if requested by service provider. This field is not used in the Juniper ATP Cloud, hence retain the default value.
SAML Issuer ID	SAML IdP Issuer ID This field is not used in the Juniper ATP Cloud, hence retain the default value.

Table 89: SSO SAML Settings for Okta *(Continued)*

Field	Description
Attribute Statements	When you create a new SAML integration, or modify an existing one, you can define custom attribute statements. These statements are inserted into the SAML assertions shared with Juniper ATP Cloud. 1. Name — the reference name of the attribute. The maximum length is 512 characters. The Name attribute must be unique across all user and group attribute statements. It is where you specify the mapping for Juniper ATP Cloud. Example, • firstname (optional) • lastname (optional) • username (mandatory) **NOTE**: The username attribute is mandatory for Juniper ATP Cloud. It is used for logging in to Juniper ATP Cloud portal. 2. Name Format — the format of the name attribute. The supported formats are: a. Unspecified —can be any format defined by the Okta profile and must be interpreted by your application. b. URI Reference —the name is provided as a Uniform Resource Identifier string. c. Basic —a simple string; the default if no other format is specified. 3. Value — the value for the attribute defined by the Name element. Admins can create custom expressions (using Okta Expression Language) to reference values in the Okta user profile. The maximum length for this field is 1024 characters. Sample attribute statement is provided in Table 90 on page 254.

Table 89: SSO SAML Settings for Okta *(Continued)*

Field	Description
Group Attribute Statements (optional)	If your Okta org uses groups to categorize users, you can add group attribute statements to the SAML assertion shared with your application. User's groups is mapped to the attribute statement in the SAML Response. The group attribute helps in identifying which user belongs to which group. 1. Enter the name of the group attribute in your SAML app. example: role 2. Select a Name Format. 3. Choose a Filtering option for your expression: Starts with, Equals, Contains, or Matches regex 4. Type in the expression that will be used to match against the Okta GroupName values and added to the SAML assertion. You can create group attribute for role_administrtor, role_observer, and role_operator and add users to the group. Sample group attribute statement is provided in Table 91 on page 255.
Preview the SAML assertion	Click to view the Xml file that will be used in the assertion.

Table 90: Sample Attribute Statements for Okta

Name	Name Format	Value
firstname	Unspecified	user.firstName
lastname	Unspecified	user.lastName
email	Unspecified	user.email

NOTE: The firstname and lastname attributes are optional. In Juniper ATP Cloud SSO SAML Provider Settings, you must set a mandatory field named **Username Attribute**. Whatever attribute value you have planned to set in Juniper ATP Cloud, you must set the same attribute value in Okta IdP, else SSO will fail.

For example, if you plan to set the **Username Attribute** value in the Juniper ATP Cloud SSO SAML Provider Settings to **user.email**, then you must set the same attribute in Okta IdP with the attribute value as **user.email**.

Table 91: Sample Group Attribute Statements for Okta

Name	Name Format	Filter	
role	Unspecified	contains	role

Table 92: Sample Role Mapping in Okta

Role Mapping in Okta	Role Mapping in Juniper ATP Cloud Portal
role_administrator	Set Administrator field to role_administrator when you configure SSO settings in Juniper ATP Cloud Portal.
role_operator	Set Operator field to role_operator when you configure SSO settings in Juniper ATP Cloud Portal.
role_observer	Set Observer field to role_observer when you configure SSO settings in Juniper ATP Cloud Portal.

Example: Configure SSO with Microsoft Azure as IdP

This section provides step-by-step instructions to configure SSO with Microsoft Azure as IdP:

NOTE:

- The information provided in this section is based on the current SSO with SAML implementation by Microsoft Azure and is subject to change. For more detailed information, see Microsoft Azure Documentation.

- You must already have an account with Microsoft Azure.
- You must log in as an administrator to perform the following operations.

1. Log in to Azure portal.
2. Click **Azure Active Directory > Enterprise Applications**.
3. Click **+ New application > +Create your own application**.
4. Enter the application name and click **Create**.
   The new application is listed in the All applications page.
5. Click on the application name.
6. Click **Assign users and groups > Add user/group**.
   The Add assignment page appears.
7. Click **None selected**. Choose the users and groups from the **Users and groups** list and click **Select**.

   NOTE: When you assign a group to an application, only users directly in the group will have access. The assignment does not cascade to nested groups.

8. Click **Assign**. For sample users and groups, see Table 93 on page 256
9. Navigate to **Manage > Single Sign-on > SAML**. Configure the settings as per the guidelines provided in Table 94 on page 257.
10. Click **Test** to check if SSO is working.

    NOTE: You must add users to Users and groups before you can sign in.

11. Navigate to **Security > Token encryption > Import Certificate** and upload the encryption certificate. IdP administrator must generate and upload the certificate to enable token encryption

Table 93: Sample Users and Group Settings for Microsoft Azure

Display Name	Object Type	Role Assigned
role_administrator	Group	User

Table 93: Sample Users and Group Settings for Microsoft Azure *(Continued)*

Display Name	Object Type	Role Assigned
role_observer	Group	User
role_operator	Group	User

Table 94: SSO Settings for Microsoft Azure

Field	Description
Basic SAML Configuration	
Identifier (Entity ID)	(Mandatory) The default identifier will be the audience of the SAML response for IDP-initiated SSO. This value must be unique across all applications in your Azure Active Directory tenant Example: *https://amer.sky.junipersecurity.net*
Reply URL (Assertion Consumer Service URL)	(Mandatory) The default reply URL will be the destination in the SAML response for IDP-initiated SSO. The reply URL is where the application expects to receive the authentication token. This is also referred to as the “Assertion Consumer Service” (ACS) in SAML. Example: *https://amer.sky.junipersecurity.net/portal/sso/acs*
Sign on URL	(Optional) This URL contains the sign-in page for this application that will perform the service provider-initiated SSO. Leave it blank if you want to perform IdP initiated SSO.
Relay State	(Optional) The relay state instructs the application where to redirect users after authentication is complete, and the value is typically a URL or URL path that takes users to a specific location within the application. The value in this form only takes effect in an IdP-initiated SSO flow. Juniper ATP Cloud does not support IdP-initiated SSO. We recommend you leave this field blank.
User Attributes & Claims Parameters that define which access control groups to associate with ATP. The access control groups are mapped to Juniper ATP roles.	

Table 94: SSO Settings for Microsoft Azure *(Continued)*

Field	Description
Unique User Identifier	(Optional) Provide the Name ID. Example: user.userprincipalname [nameid-format:emailAddress]
+Add new claim	Define the claims used by Azure AD to populate SAML tokens issued to Juniper ATP Cloud. To add a new claim: 1. Click **+ Add new claim**. The Manage claim page appears. 2. Enter the claim name and namespace. 3. Select the source. 4. Select the source attribute from the drop-down list. 5. (Optional) Specify the claim condition. 6. Click **Save**. See Table 95 on page 261. **NOTE**: The givenname and surname attributes are optional. In Juniper ATP Cloud SSO SAML Provider Settings, you must set a mandatory field named **Username Attribute**. Whatever attribute value you have planned to set in Juniper ATP Cloud, you must set the same attribute value in Azure IdP, else SSO will fail. For example, if you plan to set the **Username Attribute** value in the Juniper ATP Cloud SSO SAML Provider Settings to **emailaddress**, then you must set the same attribute name in Azure IdP with the attribute value as **user.mail**.

Table 94: SSO Settings for Microsoft Azure *(Continued)*

Field	Description
+ Add a group claim	Define the group claims used by Azure AD to populate SAML tokens issued to Juniper ATP Cloud. To add a new group claim: 1. Click **+ Add a group claim**. The Group Claims page appears. 2. For groups associated with users, choose **All groups**. 3. Select the source attribute. • If the source attribute is sAMAccountName, then you must specify the role name as the attribute for role mapping in Juniper ATP Cloud portal. For example, role: role_administrator • If the source attribute is Group ID, then you must specify the reference ID as the attribute for role mapping in Juniper ATP Cloud portal. For example, role: abcdef **NOTE**: • The source attribute only works for groups synchronized from an on-premises Active Directory using AAD Connect Sync 1.2.70.0 or above. • If you do not have the Azure Active Directory (AD) to pull the users and groups, then choose Group ID as the source attribute in the Azure IdP and provide the respective group ID in Juniper ATP Cloud SSO setting group attributes. 4. Select the **Customize the name of the group** check box. 5. Specify the name and namespace. For example, if the group name is role, then in the SAML response to Juniper ATP Cloud, the group name "role" will be the key and the value of the key will be the role name, where the users are added. 6. Click **Save**. Group claim role is created with value as user.groups.
SAML Signing Certificate	
Status	Displays the status of the SAML certificate used by Azure AD to sign SAML tokens issued to your application.

Table 94: SSO Settings for Microsoft Azure *(Continued)*

Field	Description
Thumbprint	Displays the thumbprint of the SAML certificate.
Expiration	Displays the expiration date of the SAML certificate.
Notification Email	Displays the notification e-mail address.
App Federation Metadata Url	Displays the Azure IdP metadata URL for SAML. Example: https://login.microsoftonline.com/ff08d407-69c4-4850-9af0-29034d31ab36/federationmetadata/2007-06/federationmetadata.xml?appid=6915f8ab-640a-4e1c-bb67-5e81a14f7898
Certificate (Base64)	(Optional) Click to download the Base64 certificate.
Certificate (Raw)	(Optional) Click to download the Raw certificate.
Federation Metadata XML	(Optional) Click to download the federation metadata document.
Signature Algorithm	Determines the signing algorithm used to digitally sign the SAML assertion and response. Azure provides RSA-SHA256 signature algorithm.
Set up Application (Juniper ATP Cloud)	
Login URL	Displays the login URL for Microsoft Azure. You will be redirected to login URL for authentication. Example: https://login.microsoftonline.com/ff08d407-69c4-4850-9af0-29034d31ab36/saml2

Table 94: SSO Settings for Microsoft Azure *(Continued)*

Field	Description
Azure AD Identifier	Displays the intended audience of the SAML assertion. It is the Entity ID (a globally unique identifier) of Azure IdP. Example: https://sts.windows.net/ff08d407-69c4-4850-9af0-29034d31ab36/
Logout URL	Displays the logout URL for Microsoft Azure This field is not yet supported in Juniper ATP Cloud.

Table 95: Add New Claim for Azure AD

Attribute Name	Source Attribute Value	Description
givenname	user.givenname	The givenname attribute will be used to map last name of the user in ATP Cloud.
surname	user.surname	The surname attribute will be used to map last name of the user in ATP Cloud.
emailaddress	user.mail	
		The emailaddress attribute will be used to map email address of the user in ATP Cloud.

Step 2: Configure SSO Settings in Juniper ATP Cloud Web Portal

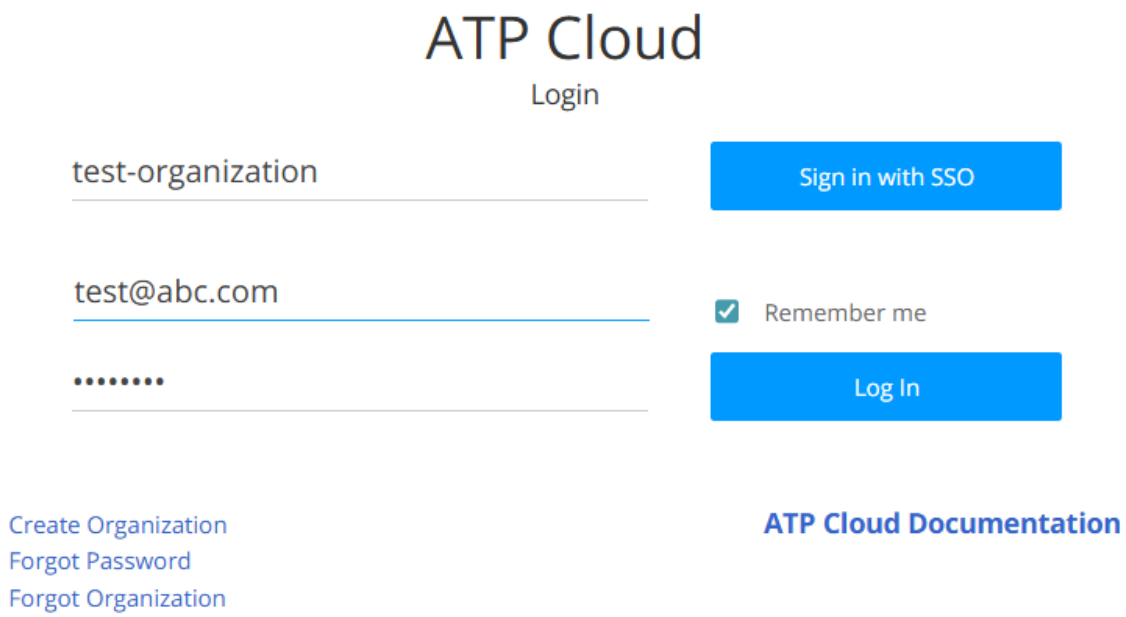
See Configure SSO Settings.

Step 3: Activate SSO Configuration

To activate SSO configuration, log in to Juniper ATP Cloud portal, navigate to **Administration** > **Single Sign-on Setting** and click **Activate**.

Step 4: Test SSO Configuration

- SSO initiated by Service Provider (Juniper ATP Cloud)—Log in to Juniper ATP Cloud Web portal with SSO. If you log into the Juniper ATP Cloud Web Portal before authenticating with IdP SSO, then based on the ATP Cloud organization, you will be redirected to the IdP portal for authentication. After authentication with IdP, you are logged in to Juniper ATP Cloud Web portal.



- Identity Provider—When you log in to the IdP SSO account, it provides a list of applications that are integrated with IdP and you can access any of the applications. For example, if you click the Juniper ATP Cloud application, you are directed to Juniper ATP Cloud Web portal.

Troubleshoot SSO Configuration

Use the following information to troubleshoot errors and issues when using SAML 2.0 with Juniper ATP Cloud.

- Organization
  - The SSO setting is configured per organization. Both local and SAML users can co-exist in an organization. By default, the organization creator (administrator) is the local user.
  - If SSO fails due to incorrect configuration and SSO user is unable to login, then contact the organization creator (administrator), who has local login access to the organization. Administrator can login with the ATP Cloud customer portal URL and fix the SSO configuration for the organization.

- Role mapping
  - Juniper ATP Cloud has the 'admin', 'operator', 'observer' roles set as part of the user profiles creation use case.
  - To authenticate ATP users with IdP, you need to have at least one group in IdP that defines ATP users, which will eventually be mapped to ATP roles.
  - Users can create an IdP group for each ATP role type: 'admin', 'operator', 'observer' and map the roles appropriately during IdP configuration.
  - If the user group doesn't match with the mapping on IdP, an error message is displayed to the user.
- Multifactor authentication
  - If IdP provides its own step-up authentication capability, SSO user will be redirected to the SSO site for the step-up authentication. Multifactor Authentication on Juniper ATP Cloud is disabled if single-sign-on is enabled.
  - Local users on the same organization can continue to use ATP's multifactor authentication (MFA).
- Password
  - SSO users who have forgotten the password must log in to the IdP site to reset the password. When a user tries to SSO by providing the organization name, ATP Cloud portal will redirect the user to IdP site for the authentication. If user authentication fails in the IdP site. then the user must reset the password from the IdP site.
  - The Forgot password option in Juniper ATP Cloud portal is for the organizations that are not configured with SSO.

RELATED DOCUMENTATION

Configure SSO Settings

Configure Single Sign-On

To access this page, click **Administration** > **Single Sign-On**. You can configure, activate, or deactivate Single sign-on (SSO) from the Single Sign-On Configuration page.

The entities involved during the SSO configuration are:

- Identity Provider (IdP)—An external server that handles management of user identities. For example, Okta, and Microsoft Azure.

- Service Provider—Juniper ATP Cloud acts as a service provider that receives the SAML assertion sent by IdP in response to a login request.

Both IdP and service provider trust each other and share configurations.

Before you begin:

- See "Set Up Single Sign-on with SAML 2.0 Identity Provider" on page 248.
- Ensure that IdP is already configured with SSO SAML settings.

NOTE: You must configure the SSO setting per organization.

To configure SSO settings:

1. Select **Administration**> **Single Sign-On**.
2. Complete the configuration by using the guidelines in Table 96 on page 264.
3. Click **Save**.

After configuring the service provider settings and the IdP settings, you can activate SSO. To activate SSO, click **Activate**.

To deactivate existing SSO, click **Deactivate**.

Table 96: SSO Settings

Field	Description
Service Provider Settings	
Display Name	Enter a display name for the SSO setting.
Entity ID	Enter the unique identifier for Juniper ATP Cloud customer portal.
Username Attribute	Enter the username attribute for SAML. Username attribute is mandatory and must be in e-mail address format. The username attribute is mapped to the user data, which is provided by IdP in the SAML assertion response.

Table 96: SSO Settings *(Continued)*

Field	Description
Sign Authentication Requests	Enable the toggle button to sign the SAML authentication requests sent from Juniper ATP Cloud to IdP. If you enable sign authentication requests, you must provide both private key and public key certificate.
Encrypt SAML Response	Enable the toggle button to specify that the SAML assertion returned by the IdP is encrypted. If the encrypt SAML response is enabled, you must provide both private key and public key certificate. **NOTE**: If you have enabled encryption for SAML response in Juniper ATP Cloud customer portal but the SAML responses from your IdP are not encrypted, then SAML authentication will be rejected.
Private Key	Enter the private key. The private key is generated locally by the user. In Juniper ATP Cloud, the private key is used to sign SAML authentication request. The private key is not shared with IdP.
Public Key Certificate	Enter the public key certificate. The public key certificate is generated locally by the user. You must upload the same public key certificate in IdP portal. In IdP, the public key certificate is used to validate the SAML authentication request sent by Juniper ATP Cloud.
Role Options	Choose **Use default role** or **Enter IdP specific role**.
Use default role	

Table 96: SSO Settings *(Continued)*

Field	Description
Default Role	Select a default role for the SAML user in the organization. If you haven't entered the role under Role Mapping section, you must specify the default role for the organization. Select the default role from the list. • System Administrator—Full privileges • Operator—Full privileges but cannot create users • Observer—Read only privileges • None—No default role **NOTE**: You must configure the role attribute or the default role to log into the SSO page.
First Name	Enter the first name attribute of the SAML user. The first name attribute is used to create the user profile. If you do not provide the first name, then a part of the e-mail address is used as the first name to create the user profile.
Last Name	Enter the last name attribute of the SAML user. The last name attribute is used to create the user profile. If you do not provide the last name, then a part of the e-mail address is used as the last name to create the user profile.
Enter IdP specific role	
Group Attribute	(Optional) Enter the group attribute that is configured in IdP. Example: role
Administrator	(Optional) Enter the IdP specific role that must be mapped to the Juniper ATP Cloud Administrator role. Example: role_admin

Table 96: SSO Settings *(Continued)*

Field	Description
Operator	(Optional) Enter the IdP specific role that must be mapped to the Juniper ATP Cloud Operator role. Example: role_operator
Observer	(Optional) Enter the IdP specific role that must be mapped to the Juniper ATP Cloud Observer role. Example: role_observer
First Name	Enter the first name attribute of the SAML user. The first name attribute is used to create the user profile. If you do not provide the first name, then a part of the e-mail address is used as the first name to create the user profile.
Last Name	Enter the last name attribute of the SAML user. The last name attribute is used to create the user profile. If you do not provide the last name, then a part of the e-mail address is used as the last name to create the user profile.
Export SP Metadata	Click **Export SP Metadata** to download service provider metadata in XML format. The administrator can download and use the service provider metadata to dynamically configure all service provider settings in IdP portal, at a time. The administrator need not manually configure individual service provider settings.
Identity Provider Settings	
IdP Settings	Select **Import Settings** to import the IdP metadata in one go. To manually configure the IdP settings, select **Enter settings manually**.
Import	Select the IdP metadata in XML format and click Import.

Table 96: SSO Settings *(Continued)*

Field	Description
Entity ID	Enter the unique identifier for the IdP. If you import IdP metadata, the information will be updated automatically.
Login URL	Enter the redirect URL for user authentication in IdP. If you import IdP metadata, the information will be updated automatically.
IdP Certificate	Enter the IdP certificate to decrypt the SAML response. If you import IdP metadata, the information will be updated automatically.

RELATED DOCUMENTATION

Set Up Single Sign-on with SAML 2.0 Identity Provider | 248

View Audit Logs

Audit logs contain information about the login activity and specific tasks that were completed successfully using the ATP Cloud Web Portal. Audit log entries include details about user-initiated tasks, such as the username, task name, task details, and date and time of task execution. Administrators can view audit logs for a specific time span, search and filter for audit logs, and export audit logs in comma-separated values (CSV) format.

NOTE:

- To view audit logs, you must have Audit Log Administrator privileges.
- The retention period for audit logs is five years.

To view audit logs:

1. On the ATP Cloud Web Portal UI, select **Monitor > Audit**.

The Audit Log page appears displaying the audit logs in tabular format. The fields displayed on the Audit Log page are described in Table 97 on page 269.

2. (Optional) Click **Details** link to view the details for that audit log.

   The Audit Log Detail dialog box is displayed. This page displays additional fields that are not displayed on the Audit Log page; these fields are described in Table 98 on page 269.

   Click **OK** to close the Audit Log Detail dialog box.

3. (Optional) Click **Export** to export audit logs as a comma-separated values (CSV) file to view and analyze the exported audit logs. You can either export all audit logs at once or for a specific timespan.
4. (Optional) Click **Time Span** and select the time span to view the audit log for a specific period.

Table 97: Fields on the Audit Log Page

Field	Description
Timestamp	Timestamp for the audit log file that is stored in UTC time in the database but mapped to the local time zone of the client computer.
Username	Username of the user that initiated the task.
Action	Name of the task that triggered the audit log.
Details	Detailed information about the task performed. Click the details link to view more details about the task.

Table 98: Fields on the Audit Log Details Page

Field	Description
Timestamp	Timestamp for the audit log file that is stored in UTC time in the database but mapped to the local time zone of the client computer.
Username	Username of the user that initiated the task.
Action	Name of the task that triggered the audit log. For details, see Table 99 on page 270.

Table 99: Fields displayed for Audit Log Action

Action that triggered the Audit Log	Fields Displayed on Audit Log Details Column
Create application token	{'token id': , 'token name': , 'token description': }
Update application token	{"token id": , "token name": , "token description": }
Delete application token	{"token id": }
User login	{"role": , "client ip": , "XFF": }
User logout	{"role": , "client ip": , "XFF": }
Request enrollment slax script	{"enrolled from": }
Request disenrollment slax script	{"enrolled from": }
SRX enrollment complete (or) SRX disenrollment complete	{'serial number': , 'model': , 'version': , 'host': , 'enrolled from': }
SRX enrollment complete (or) SRX disenrollment complete	{'serial number': , 'model': , 'version': , 'host': , 'enrolled from': }
Report Threat Source server	{"cc server": , "report type": }
Create file inspection profile	{"profile name": }
Update file inspection profile	{"profile name":, "profile id": , 'category thresholds': , 'disabled categories': }
Delete file inspection profile	{"profile name": }
Create enrollment command	

Table 99: Fields displayed for Audit Log Action *(Continued)*

Action that triggered the Audit Log	Fields Displayed on Audit Log Details Column
Create disenrollment command	
Delete devices	{'devices': }
Delete device statistics data	{'devices': }
Delete device	{"device": }
Enroll device	{"device": }
Disenroll device	{"device": }
Attach device to organization	{"device": , "organization": }
Detach device from organization	{"device": , "organization": }
Administrator action on blocked attachments	{"action": , "id": }
Administrator action on quarantined emails	{"action": , "id": }
User action on blocked attachments	{"action": , "id": }
User action on quarantined emails	{"action": , "id": }
Update quarantined emails configuration	{"smtp": {}, ... }
Update blocked attachments configuration	{"imap": {}, ... }
Update blocked attachments configuration	{"server_list": }

Table 99: Fields displayed for Audit Log Action *(Continued)*

Action that triggered the Audit Log	Fields Displayed on Audit Log Details Column
Update blocked attachments configuration	{'domain_name': }
Delete blocked attachments configuration	{'domain_name': }
Update quarantined emails configuration	{'release_option': , 'release_email': , 'replacement_link_text': , 'replacement_subject': , 'replacement_body': , 'learn_more_url': }
Update blocked attachments configuration	{'notification_link_text': , 'notification_subject': , 'notification_body': , 'learn_more_url': , 'unblock_email': }
Update administrator blocked attachments notification	{'notify_email': , 'notify_block': , 'notify_unblock': }
Delete administrator blocked attachments notification	{'notify_email': , ...}
Update administrator quarantined emails notification	{'notify_email': , 'notify_quarantine': , 'notify_release': }
Delete administrator quarantined emails notification	{'notify_email': , ...}
Report Encrypted Traffic server	{"eta server": , "report type": }
Add data to Encrypted Traffic allowlist	[{"value": , } ...]
Update data of Encrypted Traffic allowlist	{"existing value": , "new value": }
Delete data from Encrypted Traffic allowlist	{"deleted value": }
Update infected host threat level threshold	{"host threshold": }

Table 99: Fields displayed for Audit Log Action *(Continued)*

Action that triggered the Audit Log	Fields Displayed on Audit Log Details Column
Update TAXII sharing threshold	{"taxii threshold": , "taxii sharing": }
Update host event and malware logging	{"host status": , "malware status": }
Update MIST integration status	{"mist status": }
Create infected host email configuration	{"email": , "email threshold":}
Update infected host email configuration	{"email": , "email threshold": }
Delete infected host email configuration	{"email": }
Add data to hash	{'valid hashes': ,'unique hashes': , 'invalid hashes': }
Replace data of hash	{'valid hashes': ,'unique hashes': , 'invalid hashes': }
Delete data from hash	{"hashes": }
Delete data from hash	{'valid_hashes': , 'invalid_hashes': }
Update host investigation status	{"host ip": , "inv status": , "policy": , "label": }
Update host investigation status	{"host ip": , "inv status": , "policy": , "label": }
Log host tracking records	
Update SecIntel third party feed configuration	{"feeds": [{"feed_name": , "feed_in_ha": }, ...]}
Request password reset	

Table 99: Fields displayed for Audit Log Action *(Continued)*

Action that triggered the Audit Log	Fields Displayed on Audit Log Details Column
Successful password reset	
Update proxies	{'proxy ips': }
Delete proxies	{'proxy ips': }
Create organization	{"organization": }
Delete organization event data	{"organization": }
Add data to C&C Server [allowlist|blocklist]	[{'value': ,'user_comments':}, ...]
Delete data from C&C Server [allowlist|blocklist]	[{'value': ,'user_comments':}, ...]
Add data to C&C Server [allowlist|blocklist]	{"file name": , "data": }
Delete data from C&C Server [allowlist|blocklist]	{"file name": , "data": }
Update data of C&C Server [allowlist|blocklist]	{"entry id": , "value": }
Delete data from C&C Server [allowlist|blocklist]	{"entry": , "value": , "last_updated": , "user_comments": , "submitted_by": }
Report file submission	{"submission id": , "report type": , 'already submitted': }
User manually uploaded file	{"submission id": , "user comments": , "file name": , "already submitted": , "threat level": }
Create user profile	{'first_name': , 'last_name': , "username": }
Update user profile	{'first_name': , 'last_name': , "username": }

Table 99: Fields displayed for Audit Log Action *(Continued)*

Action that triggered the Audit Log	Fields Displayed on Audit Log Details Column
Update user profile	{'first_name': , 'last_name': , "username": }
Update user profile	{'first_name': , 'last_name': , "username": }
Update user profile	{'first_name': , 'last_name': , "username": }
Delete user profile	{"username": }
Change user password	
Submit user feedback	{"feedback_type": }
Add data to [URL| IP] [allowlist|blocklist]	{"added_values": }
Update data of [allowlist|blocklist]	{"previous value": , "new value": }
Delete data from [allowlist|blocklist]	{"deleted value": }
Replace [allowlist|blocklist] data	{"data": [{'value': }, ...]}
Replace [allowlist|blocklist] data	{"data": [{'value': }, ...]}
Update [allowlist|blocklist] data	{operation: } operation can be 'add' or 'remove'
Update [allowlist|blocklist] data	{operation: } operation can be 'add' or 'remove'
Update [allowlist|blocklist]data	{operation: } operation can be 'add' or 'remove'
Update [allowlist|blocklist] data	{operation: } operation can be 'add' or 'remove'

Table 99: Fields displayed for Audit Log Action *(Continued)*

Action that triggered the Audit Log	Fields Displayed on Audit Log Details Column
Update [allowlist|blocklist] data	{operation: , "file name": } operation can be 'add' or 'remove'
Update [allowlist|blocklist] data	{operation: , "file name": } operation can be 'add' or 'remove'
User logged in	{"role": , "client ip": , "XFF": }
SRX initiated enrollment	{"version": , "model": , "organization": }
SRX initiated disenrollment	{"version": , "model": , "organization": }
Delete device	{"device": }
Delete device	{"devices": }
Update infected host expiration	data = {"expiry config": , "ips": [{"value": }, ...] }
Update Multifactor Authentication	{"mfa method": , "mfa period": }
Request Multifactor Authentication Code	{"mfa_method":}
Verify Multifactor Authentication Code	
Request MFA OTP Change	
Enforce MFA OTP Change	
Request MFA OTP Enrollment	
Enforce MFA OTP Enrollment	

Table 99: Fields displayed for Audit Log Action *(Continued)*

Action that triggered the Audit Log	Fields Displayed on Audit Log Details Column
Delete MFA OTP	
Request MFA OTP reset	
Enforce MFA OTP reset	
Update phone number of a user	{"phone": }
Verify updated phone number	
Add new phone number	{"phone": }
Verify new phone number	
Delete user phone number	
Attach organization	{"organization": ,"associated organization": }
Detach organization	{"organization": ,"disassociated organization": }
Create report	{ {"reports_api": , ...}, "report_id": }
Create report definition	{"duration": , "recurrence": , "name": , "definition type":}
Update report definition	{"name": , "type": , "duration": , "recurrence": }
Delete report definition	{"name": }
Delete report	{"report id": }

Table 99: Fields displayed for Audit Log Action *(Continued)*

Action that triggered the Audit Log	Fields Displayed on Audit Log Details Column
Create adaptive threat profiling feed	{"feed type": , "ttl": , "infected host feed": , "feed category": , "feed name": }
Delete excluded adaptive threat profiling feed entry	{"delete entry": }
Add excluded adaptive threat profiling feed entry	{"feed name": , "added entry": }
Add user excluded adaptive threat profiling feed entry	{"feed name": , "added entry": }
Update adaptive threat profiling feed	{"ttl": , "infected host feed": , "feed name": }
Delete adaptive threat profiling feed	{"feed name": }

NOTE: If the value of the field is none, then that field is not displayed on the Audit Log Details page

RELATED DOCUMENTATION

Hosts Overview | 75

Host Details | 79

PART 7

More Documentation

CHAPTER 26

Additional Documentation on Juniper.net

IN THIS CHAPTER

Links to Documentation on Juniper.net

- For more information, visit the Juniper Advanced Threat Prevention Cloud Documentation page in the Juniper Networks TechLibrary.
- For information about configuring the SRX Series with ATP Cloud using the available CLI commands, see Junos CLI Reference Guide.
- For troubleshooting information, see Juniper ATP Cloud Troubleshooting Overview.
- For Internet of Things (IoT) device discovery and classification on your security device, see Security IoT User Guide.
- For information about Juniper Security Director, Juniper Security Director Cloud and Juniper Secure Edge, visit Juniper Security Director, Juniper Security Director Cloud, and Juniper Secure Edge pages in the Juniper Networks TechLibrary.
- For more information about configuring Anti-malware and SecIntel policies using J-Web, see J-Web User Guide for SRX Series Devices.
- For information about the SRX Series Firewall, visit the SRX Series Services Gateways page in the Juniper Networks TechLibrary.