JUNIPER NETWORKS | Engineering Simplicity

Quick Start

Advanced Threat Prevention Cloud

IN THIS GUIDE

Step 1: Begin

IN THIS SECTION

In this guide, we provide a simple, three-step path, to quickly get you up and running with Juniper Networks® Advanced Threat Prevention Cloud (Juniper ATP Cloud). We've simplified and shortened the configuration procedures and included how-to videos that show you how to obtain your ATP license, how to configure SRX Series Firewalls for Juniper ATP Cloud, and how to use the Juniper ATP Cloud Web Portal to enroll your SRX Series Firewalls and configure basic security policies.

Meet Juniper ATP Cloud

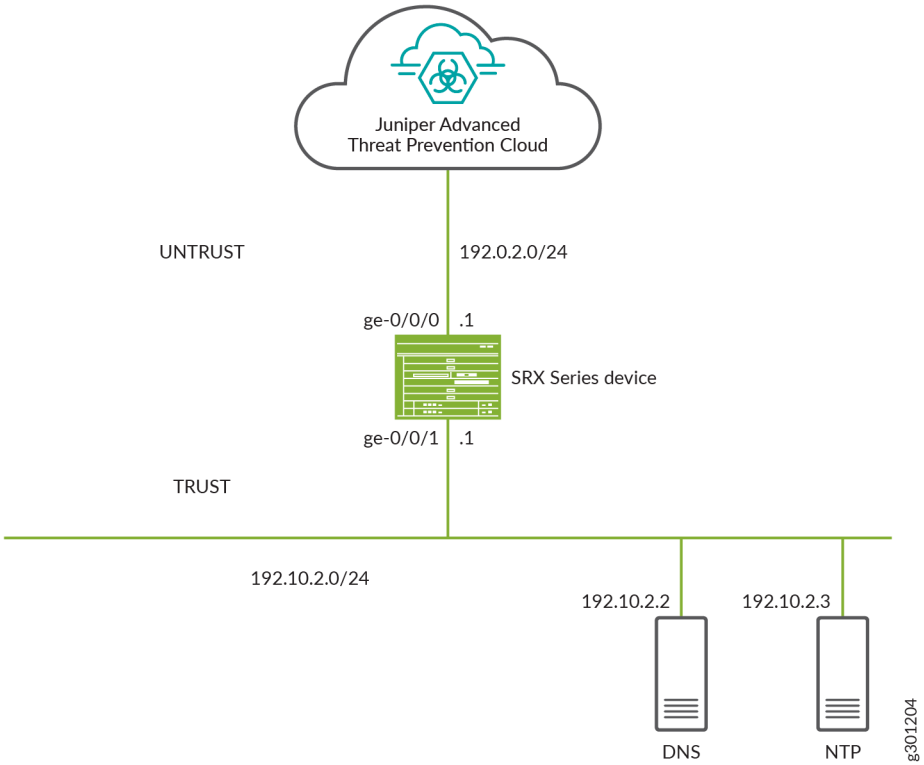
Juniper ATP Cloud is cloud-based threat detection software that protects all hosts in your network against evolving security threats. Juniper ATP Cloud uses a combination of static and dynamic analysis and machine learning to quickly identify unknown threats, either downloaded from the Web or sent through email. It delivers a file verdict and risk score to the SRX Series firewall which blocks the threat at the network level. In addition, Juniper ATP Cloud delivers security intelligence (SecIntel) feeds consisting of malicious domains, URLs, and IP addresses gathered from file analysis, Juniper Threat Labs research, and highly reputable third-party threat feeds. These feeds are collected and distributed to SRX Series firewalls to automatically block command-and-control (C&C) communications.

Want to see how Juniper ATP Cloud works? Watch now:

Video: Juniper Network's Advanced Threat Prevention Cloud

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

First things, first. You'll need to get your Juniper ATP Cloud license before you can start configuring Juniper ATP Cloud on your firewall device. Juniper ATP Cloud has three service levels: free, basic, and premium. The free license provides limited functionality and is included with the base software. Contact your local sales office or Juniper Networks partner to place an order for a Juniper ATP Cloud premium or basic license. Once the order is complete, an activation code is sent to you by email. You'll use this code in conjunction with your SRX Series Firewall serial number to generate a premium or basic license entitlement. (Use the `show chassis hardware` CLI command to find the serial number of the SRX Series Firewall).

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 License Management and vSRX Deployments. After the license is generated and applied to a specific vSRX Virtual Firewall device, use the `show system license` CLI command to view the software serial number of the device.

Want to see how to obtain a license? Watch this video:

Video: Obtain a License for Juniper ATP Cloud

Get Your SRX Series Firewall Ready to Work with Juniper ATP Cloud

After you've obtained a Juniper ATP Cloud license, you'll need to configure your SRX Series Firewall to communicate with the Juniper ATP Cloud Web Portal. Then you can configure policies on the SRX Series Firewall that use Juniper ATP Cloud cloud-based threat feeds.

NOTE: This guide assumes that you are already familiar with Junos OS CLI commands and syntax, and have experience with administering SRX Series Firewalls.

Before you begin, make sure you have an SSH connection to an Internet-connected SRX Series Firewall.

These SRX Series Firewalls support Juniper ATP Cloud:

- SRX300 line of devices

- SRX550
- SRX1500
- SRX1600
- SRX2300
- SRX4000 line of devices
- SRX5000 line of devices
- vSRX Virtual Firewall

> **NOTE**: For SRX300, SRX320, SRX340, SRX345, SRX380 and SRX550 firewalls, as part of initial device configuration, you must run `set security forwarding-process enhanced-services-mode` and reboot the device.

Let's get started and configure interfaces and security zones.

1. Set root authentication.

```
user@host# set system root-authentication plain-text-password

New password:

Retype new password:
```

> **NOTE**: The password is not displayed on the screen.

2. Set the system hostname.

```
user@host# set system host-name user@host.example.com
```

3. Set up interfaces.

```
user@host# set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.1/24

user@host# set interfaces ge-0/0/1 unit 0 family inet address 192.10.2.1/24
```

4. Configure security zones.

   The SRX Series Firewall is a zone-based firewall. You'll need to assign each interface to a zone to pass traffic through it. To configure security zones, enter the following commands:

> **NOTE**: For the untrust or internal security zone, enable only the services required by the infrastructure for each specific service.

```
user@host# set security zones security-zone untrust interfaces ge-0/0/0.0
```

```
user@host# set security zones security-zone trust interfaces ge-0/0/1.0

user@host# set security zones security-zone trust host-inbound-traffic system-services all

user@host# set security zones security-zone trust host-inbound-traffic protocols all
```

5. Configure DNS.

```
user@host# set system name-server 192.10.2.2
```

6. Configure NTP.

```
user@host# set system processes ntp

user@host# set system ntp boot-server 192.10.2.3

user@host# set system ntp server 192.10.2.3

user@host# commit
```

Step 2: Up and Running

IN THIS SECTION

Create a Web Portal Login Account for Juniper ATP Cloud

Now that you've got the SRX Series Firewall ready to work with Juniper ATP Cloud, let's log in to the Juniper ATP Cloud Web Portal and enroll your SRX Series Firewall. You'll need to create a Juniper ATP Cloud Web Portal login account, and then enroll your SRX Series Firewall in Juniper ATP Cloud Web Portal.

Have the following information handy before you start enrollment:

- Your single sign-on or Juniper Networks Customer Support Center (CSC) credentials.
- A security realm name. For example, Juniper-Mktg-Sunnyvale. Realm names can contain only alphanumeric characters and the dash ("—") symbol.
- Your company name.
- Your contact information.

- An email address and password. This will be your login information to access the Juniper ATP Cloud management interface.

Let's get going!

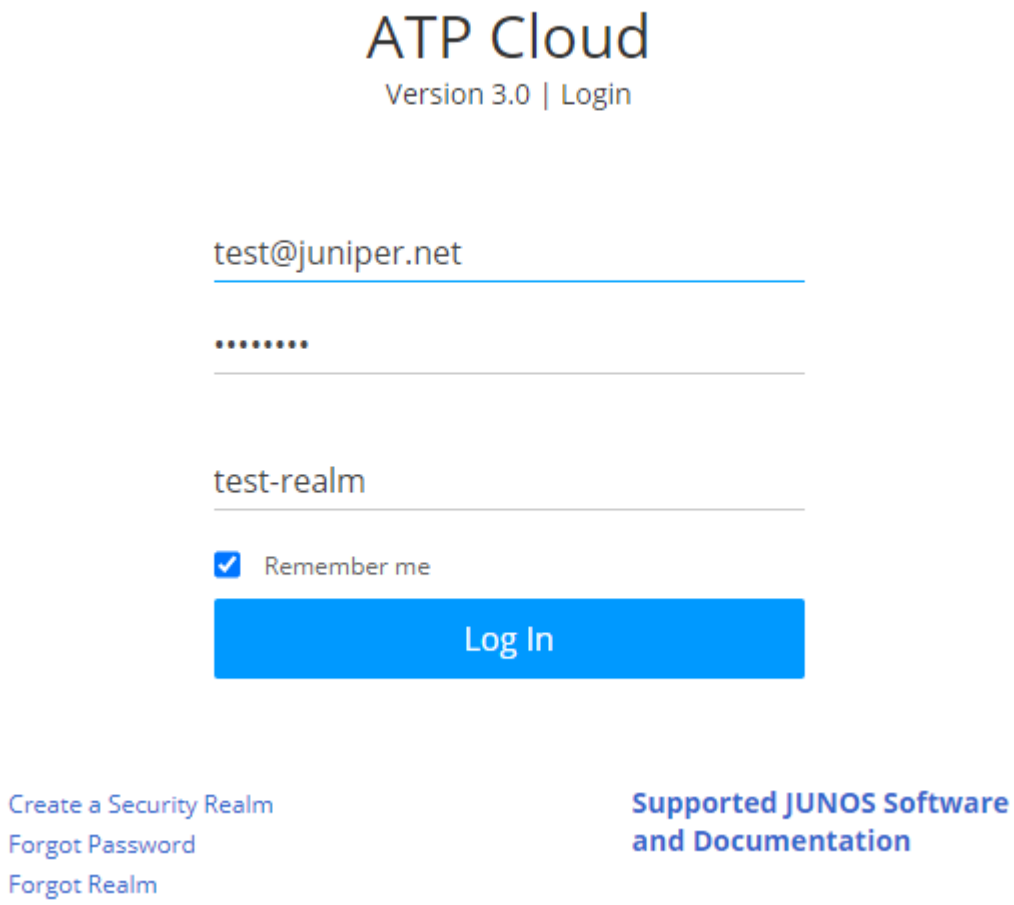
1. Open a Web browser and connect to the Juniper ATP Cloud Web Portal at https://sky.junipersecurity.net. Select your geographical region— North America, Canada, European Union, or Asia Pacific and click **Go**.

   You can also connect to the ATP Cloud Web Portal using the customer portal URL for your location as shown below.

   Table 1: Customer Portal URLs

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

   The login page opens.



2. Click **Create a Security Realm**.
3. Click **Continue**.
4. To create the security realm, follow the wizard on the screen to enter the following information:
   - Your single sign-on or Juniper Networks Customer Support Center (CSC) credentials
   - A security realm name
   - Your company name
   - Your contact information
   - The login credentials for logging into ATP Cloud
5. Click **OK**.

   You are automatically logged in and returned to the Juniper ATP Cloud Web Portal. The next time you visit the Juniper ATP Cloud Web Portal, you can log in using the credentials and security realm you just created.

Enroll Your SRX Series Firewall

Now that you've created an account, let's enroll your SRX Series Firewall in Juniper ATP Cloud. In this guide, we show you how to enroll your device using the Juniper ATP Cloud Web Portal hosted by Juniper. However, you can also enroll your device using the Junos OS CLI, the J-Web Portal, or the Junos Space Security Director Web Portal. Choose the configuration tool that's right for you:

- **Juniper ATP Cloud Web Portal**—The ATP Cloud Web Portal is hosted by Juniper Networks in the cloud. You don't need to download or install Juniper ATP Cloud on your local system.
- **CLI commands**—Starting in Junos OS Release 19.3R1, you can enroll a device to the Juniper ATP Cloud using the Junos OS CLI on your SRX Series Firewall. See Enroll an SRX Series Firewall Using the CLI.
- **J-Web Portal**—The J-Web Portal comes preinstalled on the SRX Series Firewall and can also be used to enroll an SRX Series Firewall to Juniper ATP Cloud. For details, watch this video:

  Video: ATP Cloud Web Protection Using J-Web

- **Security Director Policy Enforcer**—If you are a licensed Junos Space Security Director Policy Enforcer user, you can use Security Director Policy Enforcer to set up and use Juniper ATP Cloud. For more information about using Security Director with Juniper ATP Cloud, see How to Enroll Your SRX Series Firewall in Juniper Advanced Threat Prevention (ATP) Cloud Using Policy Enforcer.

When you enroll an SRX Series Firewall, you establish a secure connection between the Juniper ATP Cloud server. Enrollment also:

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

  NOTE: You can enroll SRX1600 and SRX2300 firewalls with Trusted Platform Module (TPM)-based certificates for TLS-based authentication and a secure connection with the Juniper ATP Cloud. For more information about TPM, see Encryption with Trusted Platform Module. Since the TPM-based certificates are used for connections between the SRX Series Firewall and Juniper ATP Cloud, you must allow traffic to the junipersecurity.net domain on ports 8444 and 7444.

- Creates local certificates
- Enrolls local certificates with the cloud server

NOTE: Juniper ATP Cloud requires that both your Routing Engine (control plane) and Packet Forwarding Engine (data plane) are connected to the Internet. You don't need to open any ports on the SRX Series Firewall to communicate with the cloud server. However, if you have a device in between, such as a firewall, then that device must have ports 80, 8080, and 443 open.

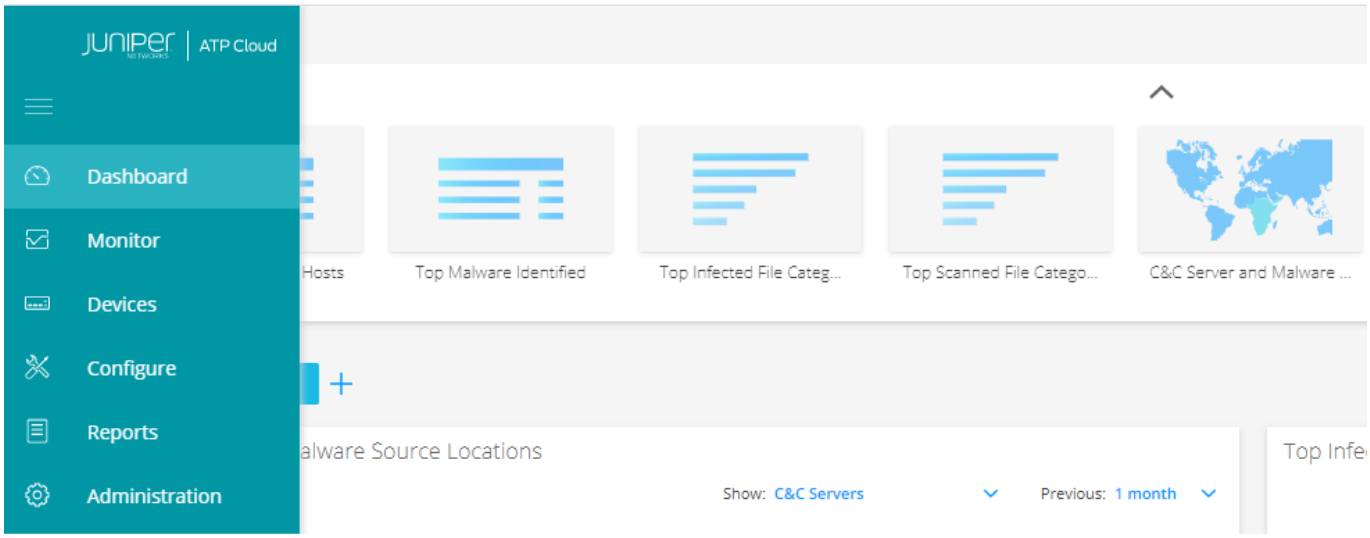
Also, the SRX Series Firewall must be configured with DNS servers in order to resolve the cloud URL.

Enroll Your SRX Series Firewall in Juniper ATP Cloud Web Portal

Here's how to enroll your SRX Series Firewall in Juniper ATP Cloud Web Portal:

1. Log in to the Juniper ATP Cloud Web Portal.

   The Dashboard page displays.



2. Click **Devices** to open the Enrolled Devices page.
3. Click **Enroll** to open the Enroll page.
4. Based on the Junos OS version that you are running, copy the CLI command from the page and run the command on the SRX Series Firewall to enroll it.

   NOTE: You must run the `op url` command from operational mode. Once generated, the `op url` command is valid for 7 days. If you generate a new `op url` command within that time period, the old command is no longer valid. (Only the most recently generated `op url` command is valid.)

5. Log in to your SRX Series Firewall. The SRX Series CLI opens on your screen.
6. Run the `op url` command that you previously copied from the pop-up window. Simply paste the command into the CLI and press Enter.

   The SRX Series Firewall will make a connection to the ATP Cloud server and begin downloading and running the op scripts. The status of the enrollment appears on screen.
7. (Optional) Run the following command to view additional information:

   ```
   request services advanced-anti-malware diagnostics customer-portal detail
   ```

   Example

   ```
   request services advanced-anti-malware diagnostics amer.sky.junipersecurity.net detail
   ```

   You can use the `show services advanced-anti-malware status` CLI command on your SRX Series Firewall to verify that a connection has been made to the cloud server from the SRX Series Firewall. After it's enrolled, the SRX Series Firewall communicates with the cloud through multiple, persistent connections established over a secure channel (TLS 1.2). The SRX Series Firewall is authenticated using SSL client certificates.

Enroll Your SRX Series Firewall in J-Web Portal

You can also enroll an SRX Series Firewall to Juniper ATP Cloud using J-Web. This is the Web interface that comes up on the SRX Series Firewall.

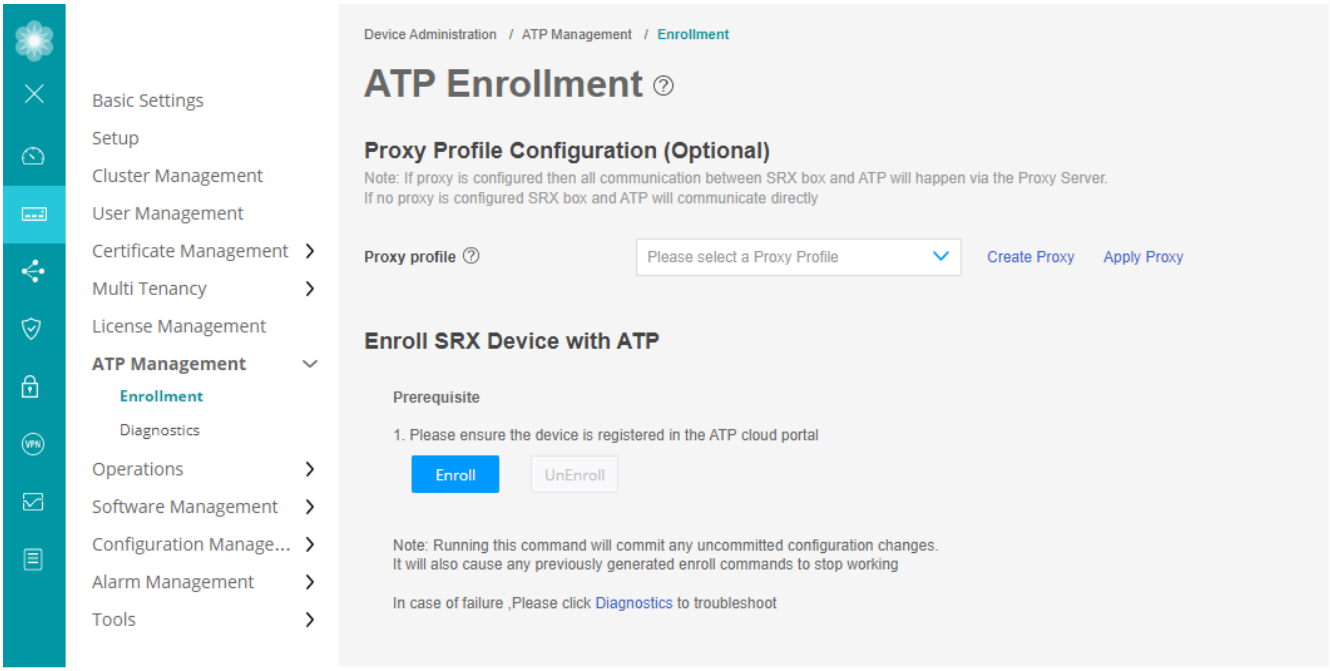
Before enrolling a device:

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

Here's how 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 opens.



   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.

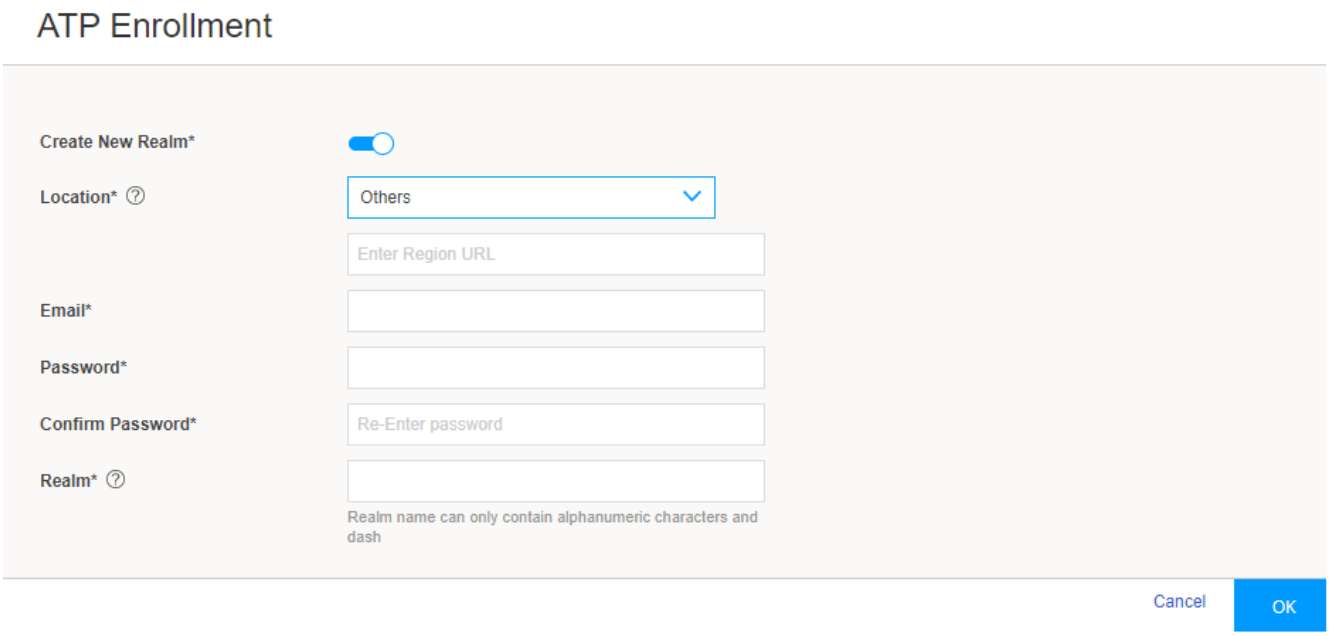
c. Click **Apply Proxy**.

  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; no spaces are allowed, 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 should be a name that is 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.

Configure Security Polices on the SRX Series Firewall to Use Cloud Feeds

Security policies, such as anti-malware and security-intelligence policies, use Juniper ATP Cloud threat feeds to inspect files and quarantine hosts that have downloaded malware. Let's create a security policy, `aamw-policy`, for an SRX Series Firewall.

1. Configure the anti-malware policy.

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

user@host# set services advanced-anti-malware policy aamw-policy http inspection-profile default

user@host# set services advanced-anti-malware policy aamw-policy http action permit

user@host# set services advanced-anti-malware policy aamw-policy http notification log

user@host# set services advanced-anti-malware policy aamw-policy smtp inspection-profile default

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

user@host# set services advanced-anti-malware policy aamw-policy imap inspection-profile default

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

user@host# set services advanced-anti-malware policy aamw-policy fallback-options notification log

user@host# set services advanced-anti-malware policy aamw-policy default-notification log

user@host# commit
```

2. (Optional) Configure the anti-malware source interface.

   The source interface is used to send files to the cloud. If you configure the source-interface but not the source-address, the SRX Series Firewall uses the IP address from the specified interface for connections. If you are using a routing instance, you must configure the source interface for the anti-malware connection. If you are using a nondefault routing instance, you don't have to complete this step on the SRX Series Firewall.

```
user@host# set services advanced-anti-malware connection source-interface ge-0/0/2
```

   NOTE: For Junos OS Release 18.3R1 and later, we recommend that you use a management routing instance for fxp0 (dedicated management interface to the routing-engine of the device) and the default routing instance for traffic.

3. Configure the security-intelligence policy.

```
user@host# set services security-intelligence profile secintel_profile category CC

user@host# set services security-intelligence profile secintel_profile rule secintel_rule match threat-level [ 7 8 9 10 ]

user@host# set services security-intelligence profile secintel_profile rule secintel_rule then action block drop

user@host# set services security-intelligence profile secintel_profile rule secintel_rule then log

user@host# set services security-intelligence profile secintel_profile default-rule then action permit
```

```
user@host# set services security-intelligence profile secintel_profile default-rule then log

user@host# set services security-intelligence profile ih_profile category Infected-Hosts

user@host# set services security-intelligence profile ih_profile rule ih_rule match threat-level [ 10 ]

user@host# set services security-intelligence profile ih_profile rule ih_rule then action block drop

user@host# set services security-intelligence profile ih_profile rule ih_rule then log

user@host# set services security-intelligence policy secintel_policy Infected-Hosts ih_profile

user@host# set services security-intelligence policy secintel_policy CC secintel_profile

user@host# commit
```

4.

> **NOTE**: If you wish to inspect HTTPs traffic, you must optionally enable SSL-Proxy in your security policies. To configure SSL-Proxy, refer to Step 4 and Step 5.
>
> Configuring these features will impact the performance of the traffic traversing the applied security policies.

(Optional) Generate public/private key pairs and self-signed certificates, and install CA certificates.

```
user@host> request security pki generate-key-pair certificate-id ssl-inspect-ca size 2048 type rsa

user@host> request security pki local-certificate generate-self-signed certificate-id ssl-inspect-ca domain-name
www.juniper.net subject "CN=www.juniper.net,OU=IT,O=Juniper Networks,L=Sunnyvale,ST=CA,C=US" email security-admin@juniper.net

user@host> request security pki ca-certificate ca-profile-group load ca-group-name trusted-ca-* filename default
```

> **NOTE**: The internal clients must trust certificates generated by the SRX Series Firewall. Therefore, you must import the root CA as a trusted CA into client browsers. This is required for the client browsers to trust the certificates signed by the SRX Series Firewall. See Importing a Root CA Certificate into a Browser.

5. (Optional) Configure the SSL forward proxy profile (SSL forward proxy is required for HTTPS traffic in the data plane).

```
user@host# set services ssl proxy profile ssl-inspect-profile-dut root-ca ssl-inspect-ca

user@host# set services ssl proxy profile ssl-inspect-profile-dut actions log all

user@host# set services ssl proxy profile ssl-inspect-profile-dut actions ignore-server-auth-failure

user@host# set services ssl proxy profile ssl-inspect-profile-dut trusted-ca all

user@host# commit
```

6. Configure the security firewall policy.

```
user@host# set security policies from-zone trust to-zone untrust policy 1 match source-address any

user@host# set security policies from-zone trust to-zone untrust policy 1 match destination-address any

user@host# set security policies from-zone trust to-zone untrust policy 1 match application any
```

```
user@host# set security policies from-zone trust to-zone untrust policy 1 then permit application-services ssl-proxy profile-name ssl-inspect-profile-dut

user@host# set security policies from-zone trust to-zone untrust policy 1 then permit application-services advanced-anti-malware-policy aamw-policy

user@host# set security policies from-zone trust to-zone untrust policy 1 then permit application-services security-intelligence-policy secintel_policy

user@host# commit and-quit
```

Congratulations! You've completed the initial configuration for Juniper ATP Cloud on your SRX Series Firewall!

Step 3: Keep Going

IN THIS SECTION

What's Next?

Now that you have basic security intelligence and anti-malware policies in place, you'll want to explore what else you can do with Juniper ATP Cloud.

Table 2: What's Next

If you want to	Then
Specify trusted and untrusted sources for your network	See Create Allowlists and Blocklists
Configure how you'd like ATP Cloud to handle email	See Email Management Overview
Define which files to send to the cloud for inspection	See Create File Inspection Profiles
Configure advanced Juniper ATP Cloud features	See the Juniper Advanced Threat Prevention Administration Guide

General Information

Table 3: General Information

If you want to	Then
View the Juniper ATP Cloud System Administration Guide	See Juniper Advanced Threat Prevention Administration Guide
See all documentation available for Juniper ATP Cloud	Visit the Juniper Advanced Threat Prevention (ATP) Cloud Documentation page in the Juniper TechLibrary
See all documentation available for Policy Enforcer	Visit the Policy Enforcer Documentation page in the Juniper TechLibrary.
Stay up-to-date on new and changed features and known and resolved issues	See the Juniper Advanced Threat Prevention Cloud Release Notes
Troubleshoot some typical problems you may encounter with Juniper ATP Cloud	See the Juniper Advanced Threat Prevention Cloud Troubleshooting Guide

Learn with Videos

Our video library continues to grow! We've created many, many videos that demonstrate how to do everything from install your hardware to configure advanced Junos OS network features. Here are some great video and training resources that will help you expand your knowledge of Junos OS.

Table 4: Learn with Videos

If you want to	Then
View an ATP Cloud Demonstration that shows you how to setup and configure ATP Cloud	Watch the ATP Cloud Demonstration video
Learn how to use the Policy Enforcer Wizard	Watch the Using the Policy Enforcer Wizard video
Get short and concise tips and instructions that provide quick answers, clarity, and insight into specific features and functions of Juniper technologies	See Learning with Videos on Juniper Networks main YouTube page

Table 4: Learn with Videos *(Continued)*

If you want to	Then
View a list of the many free technical trainings we offer at Juniper	Visit the Getting Started page on the Juniper Learning Portal