Juniper SKY ADVANCED THREAT PREVENTION

Use the instructions in this quick start to obtain your Juniper Sky ATP license key, establish a secure connection between the Sky ATP cloud server and the SRX Series device, and configure Sky ATP policies on the SRX Series device.

1

Obtain a License

Obtain a Premium or Basic License

Contact your local sales office or Juniper Networks partner to place an order for a Sky ATP premium or basic license. Once the order is complete, an authorization code is e-mailed to you. You will use this code in conjunction with your SRX Series device 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 device.)

1. Go to https://www.juniper.net/generate_license/ and log in with your Juniper Networks Customer Support Center (CSC) credentials.
2. In the Generate Licenses list, select J Series Service Routers and SRX Series Devices.
3. Using your authorization code and SRX Series serial number, follow the instructions to generate your license key. (Note that you do not enter this license key anywhere.)

Once generated, your license key is automatically transferred to the cloud server. It can take up to 24 hours for your activation to be updated in the Sky ATP cloud server.

Note for vSRX: If you are using Sky ATP with vSRX, the license is not automatically transferred. You must install the license. See License Management and vSRX Deployments for instructions.

Obtain a Free License

The free version does not require you to generate a license. The SRX Series device only needs to be enrolled to the cloud, and it will automatically be entitled to the free version. Make sure you have a Customer Support Center (CSC) user account and go directly to the instructions in section 2. If you do not have a CSC user account, see Creating a User Account. Getting your account can take up to 24 hours.

2

Create a Sky ATP Cloud Web Portal Login Account

1. Go to https://sky.junipersecurity.net and select your region. On the next screen, click "Create a security realm."
2. Enter the following required information and continue to click Next until you are finished:
   - Your single sign-on or Juniper Networks CSC credentials.
   - A security realm name — for example, Juniper-Mktg-Sunnyvale. Realm names can only contain alphanumeric characters and the dash ("-") symbol.
   - Your contact information.
   - An e-mail address and password. This will be your login information to access the Sky ATP management interface.
3. When you click Finish, you are automatically logged in and taken to the Sky ATP Web UI dashboard.

3

Enroll SRX Series Devices with Sky ATP

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

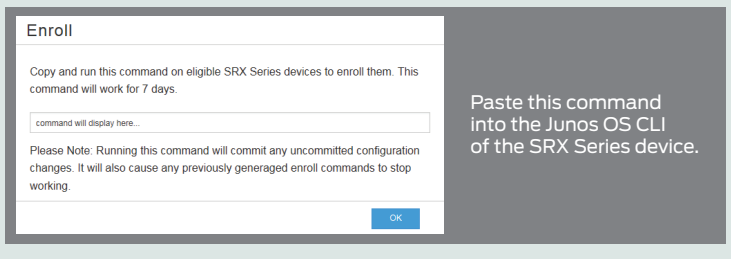
- Downloads and installs certificate authority (CAs) licenses onto your SRX Series device
- Creates local certificates and enrolls them with the cloud server
- Establishes a secure connection to the cloud server

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

1. Go to https://sky.junipersecurity.net and log in.
2. Navigate to the Devices tab in the Sky ATP Web UI and click the Enroll button.
3. Run the provided command on the SRX Series device to enroll it.

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

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



4

Configure the Advanced Anti-Malware Policy on the SRX Series Device

Note: This document assumes you are familiar with basic SRX Series device setup and configuration. For example, zone names must be configured before you proceed with the following sections. For that information, refer to the SRX Series documentation.

1. Set the policy name and enter the threshold for blocking malicious files:

   set services advanced-anti-malware policy <policy_name> verdict-threshold <number or recommended>

   Example: `set services advanced-anti-malware policy aamw_policy1 verdict-threshold recommended`

   Note: For threshold number, you can enter 1-10. If you don't know what to enter, you can use "recommended" in place of a number, and the default (7) will be used.

2. Configure an action to take when the verdict threshold for a file has been reached, and log that action:

   set services advanced-anti-malware policy <policy_name> <application> action < permit, deny> notification <log>

   Example: `set services advanced-anti-malware policy aamw_policy1 http action permit notification log`

   Note: For smtp protocol, the action is configured in the Web UI.

3. Associate the policy with the device profile so files are sent for inspection. (A default profile is shipped with Sky ATP. You can configure your own profile using the Web UI):

   set services advanced-anti-malware policy <policy_name> <protocol> inspection-profile <profile-name>

   Example: `set services advanced-anti-malware policy aamw_policy1 http inspection-profile default_profile`

4. Enable the advanced anti-malware application policy in the firewall policy:

   set security policies from-zone <zone1> to-zone <zone2> policy <firewall-policy-name> then action <permit/block> application-service advanced-anti-malware policy <policy_name>

   Example: `set security policies from-zone zone1 to-zone zone2 policy firewall-policy1 match source-address any`

   `set security policies from-zone zone1 to-zone zone2 policy firewall-policy1 match destination-address any`

   `set security policies from-zone zone1 to-zone zone2 policy firewall-policy1 match application any`

   `set security policies from-zone zone1 to-zone zone2 policy firewall-policy1 then permit application-services advanced-anti-malware-policy aamw_policy1`

5

Configure the Security Intelligence Policy on the SRX Series Device

1. Define a profile:

   set services security-intelligence profile <profile name> category Infected-Hosts

   Example: `set services security-intelligence profile ih-profile category Infected-Hosts`

2. Define rules for the profile and set the action:

   set services security-intelligence profile <profile name> rule <rule name> match threat-level [threat level]

   set services security-intelligence profile <profile name> rule <rule name> then action [action options]

   Note: Ten is the threat level category for infected hosts.

   Examples: `set services security-intelligence profile ih-profile rule secintelrule1 match threat-level 10`

   `set services security-intelligence profile ih-profile rule secintelrule1 then action permit`

3. Define the security intelligence policy and link it with the profile:

   set services security-intelligence policy <policy name> Infected-Hosts <profile name>

   Example: `set services security-intelligence policy secintel-policy1 Infected-Hosts ih-profile`

4. Enable the security intelligence policy in the firewall policy:

   set security policies from-zone <source zone name> to-zone <destination zone name> policy <firewall policy name> then permit application-services security-intelligence-policy<SecIntel policy name>

   Example: `set security policies from-zone source-zone1 to-zone dest-zone2 policy firewall-policy1 match source-address any`

   `set security policies from-zone source-zone1 to-zone dest-zone2 policy firewall-policy1 match destination-address any`

   `set security policies from-zone source-zone1 to-zone dest-zone2 policy firewall-policy1 match application any`

   `set security policies from-zone source-zone1 to-zone dest-zone2 policy firewall-policy1 then permit application-services security-intelligence-policy secintel-policy1`

What's Next?

Once you have completed this quick start, refer to the expanded documentation for the following tasks:

- Monitor and mitigate malware detections.
- Create profiles to group types of files to be scanned together under a common name. You can create multiple profiles based on the content you want scanned.
- Create policies on the SRX Series device to determine when files are sent to the cloud for inspection what to do when a file is determined to be suspicious.
- Create whitelists and blacklists to allow users to download content from trusted locations, and prevent access to content from untrusted locations.
- Update your administrator profile. You can also add additional administrator accounts.

Note: Sky ATP provides C&C and GeoIP filtering feeds that are only available with a premium or basic license. For more information on licensed features, see Sky ATP Licensing.