

Licenses for Advanced Threat Prevention

Licenses for JATP Advanced Threat Prevention Appliance

Licensing and Platform Support information

The following sections provide information on licensing requirements and SRX Series device platform support.

JATP and SRX Series Integration Licensing

Unlike other Layer 7 features, there is no separate license required on the SRX Series device for integration with JATP. In this deployment, the JATP Core is the licensed component. If the Core has a valid license, then the SRX Series device can connect to the Core and enroll successfully. If not, the enrollment will fail.

For JATP license upload instructions, see [Setting the Juniper ATP Appliance License Key](#).

Note: AppSecure functionality on the SRX Series device is a pre-requisite for integrating with JATP. Depending on the SRX Series platform, a separate license may be required to enable AppSecure. Please consult the SRX Series platform data sheet for the most accurate information.

Supported SRX Series Devices

This section describes the hardware and software components that are compatible with JATP.

Table 1 Supported SRX Series Devices

Platform	Hardware Requirements	Software Versions
vSRX Series		Junos 18.2R1 and above
SRX Series	SRX320, SRX300	Junos 18.3R1 and above
SRX Series	SRX4100, SRX4200, SRX4600	Junos 15.1X49-D65 and above for SRX4100 and SRX4200 Junos 17.4R1-S1 and above for SRX4600
SRX Series	SRX340, SRX345, SRX550m	Junos 15.1X49-D60 and above
SRX Series	SRX5800, SRX5600, SRX5400	Junos 15.1X49-D50 and above
SRX Series	SRX1500	Junos 15.1X49-D33 and above

The following devices support scanning SMTP e-mail attachments:

1. SRX300 Series device
2. SRX320 Series device
3. SRX340 Series device
4. SRX345 Series device
5. SRX1500 Series device
6. SRX4100 Series device
7. SRX4200 Series device
8. SRX4600 Series device
9. SRX5400 Series device
10. SRX5600 Series device
11. SRX5800 Series device
12. vSRX Series

The following devices support scanning IMAP e-mail attachments:

1. SRX300 Series device
2. SRX320 Series device
3. SRX340 Series device
4. SRX345 Series device
5. SRX1500 Series device
6. SRX4100 Series device
7. SRX4200 Series device
8. SRX4600 Series device
9. SRX5400 Series device
10. SRX5600 Series device
11. SRX5800 Series device
12. vSRX Series

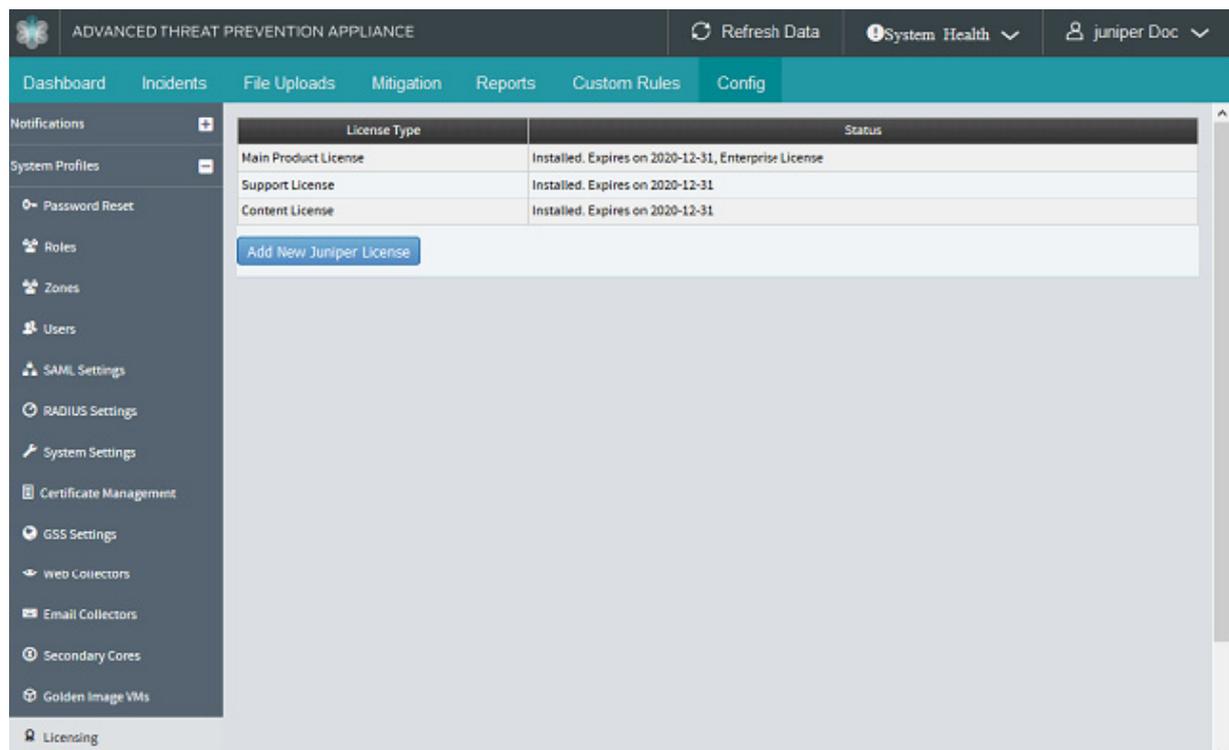
Setting the Juniper ATP Appliance License Key

Without a valid product license key, the Juniper ATP Appliance system will not work. Likewise, an expired product key, or an expired support or content license, prevents full operations and disables content or software updates.

Use the Config>System Profiles>Licensing configuration window to upload a License key to the Juniper ATP Appliance or software service. To license your system, you will need to upload the license using this configuration window and also use the CLI to get the system UUID.

Note: License Keys are obtained from Juniper Customer Support.

Figure 1 Juniper ATP Appliance License Key



To upload a product license key:

1. Navigate to the Config>System Profiles>Licensing page.
2. Click Add New Juniper ATP Appliance License button to upload a new license key file.
3. Click the Choose File button to select the license key for upload, then click Submit to apply the configuration.

Note: A GSS connection is required in order for Juniper ATP Appliance to run regular licensing checks. Adding a license manually does not enable JATPSupport.

Licenses for Juniper Advanced Threat Prevention Cloud (ATP Cloud)

Juniper Advanced Threat Prevention Cloud License Types

Juniper ATP Cloud has three service levels:

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

Note: On the Enrolled Devices page in the Juniper ATP Cloud Web UI, 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 device is disenrolled from Juniper ATP Cloud. On the SRX Series device, you can run the `> show system license` command to view license details.

Note: You do not need to download any additional software to run Juniper ATP Cloud.

Table 2 shows a comparison between the free model and the premium model.

Table 2 Comparing the Juniper ATP Cloud Free Model, Basic-Threat Feed, and Premium Model

Free Model	Basic-Threat Feeds Model	Premium Model
Management through cloud interface. Zero on-premise footprint beyond the SRX Series device.	Management through cloud interface. Zero on-premise footprint beyond the SRX Series device.	Management through cloud interface. Zero on-premise footprint beyond the SRX Series device. Also includes Encrypted Traffic Insight (ETI) and DNS security for: DGA and DNS tunnels.
Inbound protection.	Inbound protection.	Inbound protection.
Outbound protection.	Outbound protection.	Outbound protection.
—	C&C feeds.	C&C feeds.
—	GeolIP filtering.	GeolIP filtering.
—	Custom feeds	Custom feeds

Free Model	Basic-Threat Feeds Model	Premium Model
—	—	Infected host feed/endpoint quarantine
—	—	IoT Threat Prevention
—	Threat Intelligence APIs only	All APIs including File/Hash
—	—	C&C protection with event data returned to the Juniper ATP Cloud.
—	—	Compromised endpoint dashboard.
—	—	DNS security
—	—	Encrypted Traffic Insight (ETI)
Inspects only executable file types. Executables go through the entire pipeline (cache, antivirus, static and dynamic).	Inspects only executable file types. Executables go through the entire pipeline (cache, antivirus, static and dynamic).	No restrictions on object file types inspected beyond those imposed by the Juniper ATP Cloud service. You can specify which file types are sent to service for inspection.
Reporting with rich detail on malware behaviors.	Reporting with rich detail on malware behaviors.	Reporting with rich detail on malware behaviors.

For more information on analysis techniques, see [How is Malware Analyzed and Detected?](#). For additional information on product options, see the [Juniper ATP datasheet](#).

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

Additional License Requirements

AppSecure functionality on the SRX Series device is a pre-requisite for the Juniper Advanced Threat Prevention Cloud feature. Depending on the SRX Series platform, a separate license may be required to enable AppSecure. Please consult the SRX Series platform datasheet for the most accurate information.

Managing the Juniper Advanced Threat Prevention Cloud License

This topic describes how to install the Juniper ATP Cloud premium license onto your SRX Series devices and vSRX deployments. You do not need to install the Juniper ATP Cloud free license as these are included your base software. Note that the free license has a limited feature set (see [Juniper Advanced Threat Prevention Cloud License Types](#) and [File Scanning Limits](#)).

When installing the license key, you must use the license that is specific your device type. For example, the Juniper ATP Cloud premium license available for the SRX Series device cannot be used on vSRX deployments.

Obtaining the Premium License Key

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

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

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

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

[edit]

```
root@SRX# 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 Devices

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

Juniper ATP Cloud Premium Evaluation License for vSRX

The 30-day Juniper ATP Cloud countdown premium evaluation 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.

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 realm and contact information before using Juniper ATP Cloud. For more information, see [Registering a Juniper Advanced Threat Prevention Cloud Account](#).

High Availability

Before enrolling your devices with the Juniper ATP Cloud cloud, set up your HA cluster as described in your product documentation. For vSRX deployments, make sure the same license key is used on both cluster nodes. When enrolling your devices, you only need to enroll one node. The Juniper ATP Cloud cloud will recognize this is an HA cluster and will automatically enroll the other node.

Troubleshooting Juniper Advanced Threat Prevention Cloud: Checking the application-identification License

If you are using an SRX1500 Series device, you must have a have a valid application-identification license installed. Use the `show services application-identification version` CLI command to verify the applications packages have been installed. You must have version 2540 or later installed. For example:

```
user@host> show services application-identification version
Application package version: 2540
```

If you do not see the package or the package version is incorrect, use the `request services application-identification download` CLI command to download the latest application package for Junos OS application identification. For example:

```
user@host> request services application-identification download
Please use command "request services application-identification download status" to check status
```

Then use the `request services application-identification install` CLI command to install the downloaded application signature package.

```
user@host> request services application-identification install
Please use command "request services application-identification install status" to check status
```

Use the `show services application-identification application version` CLI command again to verify the applications packages is installed.

