Threat Intelligence Open API Setup Guide

Sky Advanced Threat Prevention (Sky ATP) provides the following APIs that can help you keep your network free of sophisticated malware and cyberattacks by using superior cloud-based protection:

Threat Intelligence API Overview

The Threat Intelligence open API allows you to program the Sky ATP Command and Control server (C&C) feeds to suit your requirements. You can perform the following operations using the threat intelligence API:

- Inject an IP, URL, or domain into a C&C feed with a threat level from 1 through 10. You can create up to 30 different custom C&C feeds.
  - An IP can be an IP address, IP range, or IP subnet.
  - Both IPv4 and IPv6 addresses are supported.
- Update the threat level of an IP, URL, or domain from 1 through 10.
- Delete a specific server in the feed or delete the entire feed.
- Retrieve the current status of an operation (processing) or errors (if any) from the feed processing engine.

The Threat Intelligence API supports a Swagger API specification in JSON format to allow programmatic access to it. For more information on the Swagger API specification, see https://threat-api.sky.junipersecurity.net/swagger.json.

NOTE: C&C regular feeds currently support only HTTP host URLs. For example, if you create www.example.com/example1/, it will check only www.example.com.

Blacklist and whitelist feeds (see below) support full URLs with Junos OS 15.1X49-D70 and later releases.

The following table lists the rate limits (number of requests you can make per minute) for the Threat Intelligence APIs. If you exceed these rate limits, you will receive a **429 - Too many Requests** error.

Feature	Maximum Number of Requests Per Minute
C&C feed	60
Blacklist feed	60
Whitelist feed	60

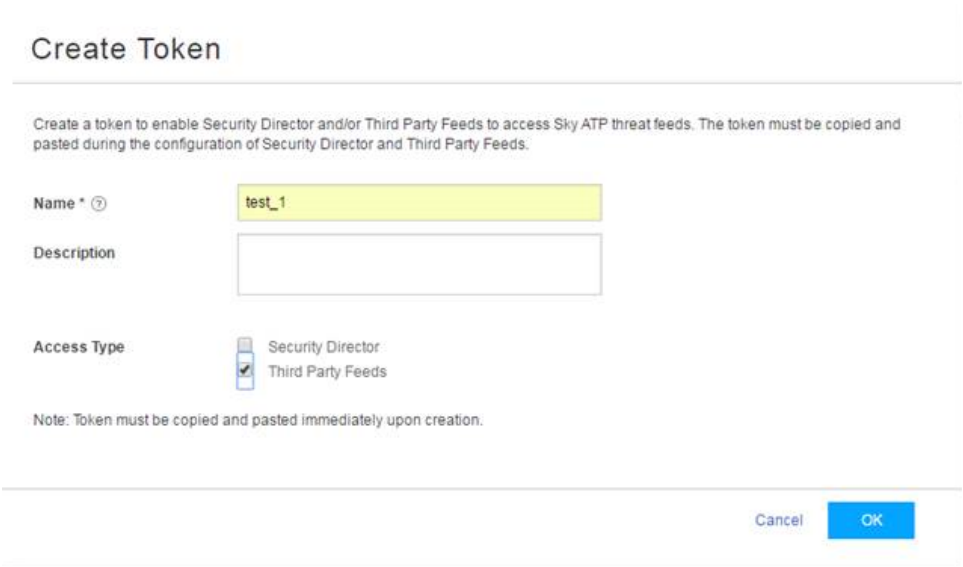
Configuration and Setup

To access the API, you must create an application token in the Sky ATP Web UI and use that token as the bearer token in the authorization header.

To generate an application token:

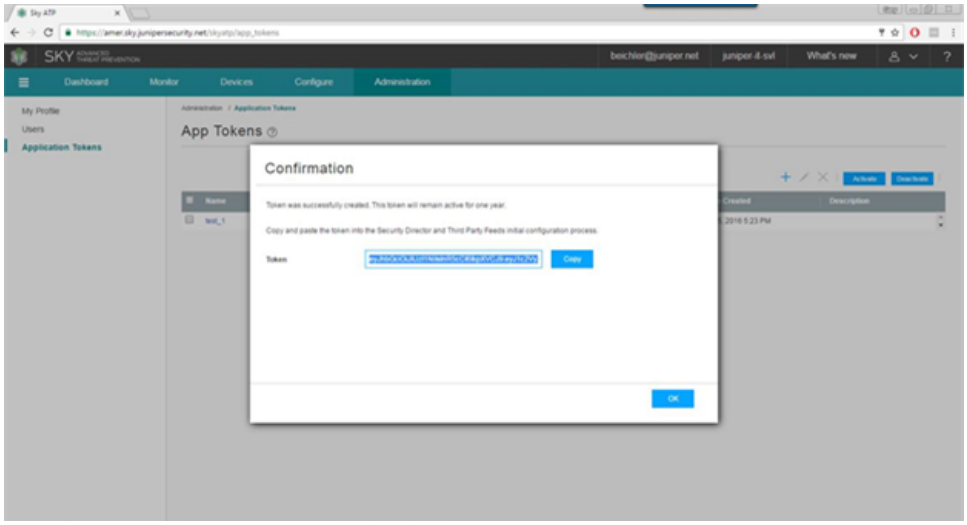
1. Log in to the Sky ATP Web UI using your credentials. Select **Administration > Application Tokens** and click the plus (+) sign. Fill in the name of the token and other required details in the pop-up box that appears and click **OK** to create a new token. See Figure 1.

Figure 1: Creating an Application Token



2. A confirmation pop-up message appears, indicating the creation of a new token, as shown in Figure 2. You can now use this token to access the Sky ATP API.

Figure 2: Confirming the Creation of an Application Token



NOTE: You can generate a maximum of 10 tokens per user, and each token is valid for one year.

For more information on how to create application tokens, see Creating Application Tokens.

Usage Examples

The following cURL examples illustrate the use of the threat intelligence API:

- **curl -k -v -XPOST -H "Authorization: Bearer <TOKEN>" -F file=@/tmp/whitelist.txt <API HOST>/v1/cloudfeeds/whitelist/file/ip/<FEEDNAME>**
- **curl -k -v -XPOST -H "Authorization: Bearer <TOKEN>" -F file=@/tmp/whitelist.txt <API HOST>/v1/cloudfeeds/cc/file/ip/<FEEDNAME>**

where:

- **API HOST** is the name of the Open API hostname corresponding to the location of the customer portal. Please refer to Table 1 for the correct hostname for your location.
- ***TOKEN*** is the application token generated in the Sky ATP Web UI.
- ***FEED NAME*** is the name of the feed you want to create.

Sky ATP API Overview

You can perform the following operations using the Sky ATP API:

- Retrieve the blacklist or whitelist for the specific server type.
- Update an IP, URL, or FQDN in a blacklist or whitelist server list.
  - An IP can be an IP address, IP range, or IP subnet.

- Both IPv4 and IPv6 addresses are supported.

- Delete a specific server in the list or delete the entire list.

The Sky ATP API supports a Swagger API specification in JSON format to allow programmatic access to it. For more information on the Swagger API specification, see https://api.sky.junipersecurity.net/swagger.json.

The following table lists the rate limits (number of requests you can make per minute) for the Sky ATP APIs. If you exceed these rate limits, you will receive a **429 - Too many Requests** error.

Feature	Maximum Number of Requests Per Minute
Hash lookup	50
File submissions	10
Blacklist	60
Whitelist	60

NOTE: Sky ATP supports up to 3,000 entries in the whitelist and 3,000 entires in the blacklist.

Configuration and Setup

To access the API, you must create an application token in the Sky ATP Web UI and use that token as the bearer token in the authorization header. See section "Configuration and Setup" on page 2 for more information on the creation of the token.

Sky ATP URLs

Sky ATP hostnames varies by location. Please refer to the following table:

Table 1: Sky ATP URLs by Location

Location	Sky ATP URL
United States	Customer Portal: **https://amer.sky.junipersecurity.net** Open API (infected hosts, whitelist/blacklist, sample submission): **https://api.sky.junipersecurity.net** Open API (threat intelligence): **https://threat-api.sky.junipersecurity.net**
European Union	Customer Portal: **https://euapac.sky.junipersecurity.net** Open API (infected hosts, whitelist/blacklist, sample submission): **https://api-eu.sky.junipersecurity.net** Open API (threat intelligence): **https://threat-api.sky.junipersecurity.net**

Table 1: Sky ATP URLs by Location (continued)

Location	Sky ATP URL
APAC	Customer Portal: **https://apac.sky.junipersecurity.net** Open API (infected hosts, whitelist/blacklist, sample submission): **https://api-apac.sky.junipersecurity.net** Open API (threat intelligence): **https://threat-api-apac.sky.junipersecurity.net**
Canada	Customer Portal: **https://canada.sky.junipersecurity.net** Open API (infected hosts, whitelist/blacklist, sample submission): **https://api-canada.sky.junipersecurity.net** Open API (threat intelligence): **https://threat-api-canada.sky.junipersecurity.net**

Usage Example

The following cURL example illustrates the use of the Sky ATP API:

- **curl -k -v -XPOST -H "Authorization: Bearer <TOKEN>" -F file=@/tmp/blacklist.txt <API HOSTNAME>/v1/skyatp/blacklist/file/ip/<FEED NAME>**

where:

- **API HOST** is the name of the Open API hostname corresponding to the location of the customer portal. Please refer to Table 1 for the correct hostname for your location.
- ***TOKEN*** is the application token generated in the Sky ATP Web UI.
- ***FEED NAME*** is the name of the feed you want to create.

File/Hash API Overview

The file/hash API lets you submit files for analysis. You can perform the following operations:

- Look up sample malware scores by hash.
- Submit samples for malware analysis.
- Update an IP, URL, or FQDN from a file in a specific list.
  - An IP can be an IP address, IP range, or IP subnet.
  - Both IPv4 and IPv6 addresses are supported.

The file/hash API supports a Swagger API specification in JSON format to allow programmatic access to it. For more information on the Swagger API specification, see https://api.sky.junipersecurity.net/swagger.json.

Configuration and Setup

To access the API, you must create an application token in the Sky ATP Web UI and use that token as the bearer token in the authorization header. See section "Configuration and Setup" on page 2 for more information on the creation of the token.

Usage Example

The following cURL example illustrates the use of the file/hash API:

- **curl -H "Authorization: Bearer<*TOKEN*>" -k <API HOSTNAME>/v1/skyatp/lookup/hash/<*SHA256*>?full_report=true**
- **curl -H "Authorization: Bearer<*TOKEN*>" -k -F file=@/srv/sample.exe <API HOSTNAME>/v1/skyatp/submit/sample**

NOTE: **API HOST is the name of the Open API hostname corresponding to the location of the customer portal. Please refer to** Table 1 **for the correct hostname for your location.**

where:

- ***TOKEN*** is the application token generated in the Sky ATP Web UI.
- ***SHA256*** is the sample hash. Only SHA256 is supported at this time.

Full reports will be completely supported in an upcoming release. The report you receive right now may slightly different in appearance and content.

Infected Host API Overview

The infected host feed is generated by Sky ATP and is used to flag compromised hosts. The feed is dynamic. Hosts are automatically added when Sky ATP suspects a host has been compromised (through a proprietary algorithm) and can be manually removed from the list through the user interface once you feel the host is no longer compromised. The feed lists the IP address or IP subnet of the host along with a threat level, for example, xxx.xxx.xxx.133 and threat level 5. This feed is unique to a realm and IP addresses within the real are assumed to be non-overlapping.

Associated with the infected host feed are a whitelist and blacklist. These are different from the generic Sky ATP whitelist and blacklist. The infected host feed uses these lists to remove hosts that are currently on an infected host feed (whitelist) and to always list a host in the infected host feed (blacklist.)

With the infected host API, you can do the following:

- Return a list of all IP addresses in the current infected host feed.
- Return a list of all IP addresses in the infected host whitelist or blacklist.

- Delete an IP address from the infected host whitelist or blacklist.
- Add an IP address to the infected host whitelist or blacklist.

The infected host API supports a Swagger API specification in JSON format to allow programmatic access to it. For more information on the Swagger API specification, see https://api.sky.junipersecurity.net/swagger.json.

Configuration and Setup

To access the API, you must create an application token in the Sky ATP Web UI and use that token as the bearer token in the authorization header. See section "Configuration and Setup" on page 2 for more information on the creation of the token.

IP Filter API Overview

A Dynamic Address Entry (DAE) provides dynamic IP address information to security policies. A DAE is a group of IP addresses, not just a single IP prefix, that can be imported. These IP addresses are for specific domains or for entities that have a common attribute such as a particular undesired location that poses a threat. The administrator can then configure security policies to use the DAE within a security policy. When the DAE is updated, the changes automatically become part of the security policy. There is no need to update the policy manually. Note that this is an IP address-only feed. It does not support URLs or fully qualified domain names (FQDNs).

The IP filter APIs let you perform the following tasks:

- Remove IP addresses (in a .csv file) from an IP filter feed
- Add IP addresses (in a .csv file) to an IP filter feed.
- Remove a specific IP address from the IP filter feed.
- Add a specific IP address to the IP filter feed.
- Remove a specific IP filter feed.
- Get the processing status of a specific IP Filter feed.

The IP filter API supports a Swagger API specification in JSON format to allow programmatic access to it. For more information on the Swagger API specification, see https://api.sky.junipersecurity.net/swagger.json.

Configuration and Setup

To access the API, you must create an application token in the Sky ATP Web UI and use that token as the bearer token in the authorization header. See section "Configuration and Setup" on page 2 for more information on the creation of the token.

Example

In this example, targeted attacked are being performed against web servers in a DMZ while concealing their identities via Tor. Tor exit nodes move frequently and keeping an up-to-date list of all 1000+ exit nodes within a firewall policy is almost impossible. This can, however, be done easily using Sky ATP's APIs. For more information on this example, see Automating Cyber Threat Intelligence with Sky ATP.

Shown below is an example script that performs the following actions:

- Polls the official TorProject's exit-node list via cURL and extracts legitimate IP information via **grep**.
- Utilizes Sky ATP's open API to install and propagate third-party threat intelligence to all SRX Series devices in the network.
- Runs on an hourly basis via cron to ensure that the active Tor Relays are always being blocked.

```
#!/bin/bash

# Define Application Token (Paste in your value between the "")
APPToken="Your_Application_Token_Here"

# Define the name of the feed you wish to create
FeedName="Tor_Exit_Nodes"

#Define temporary file to store address list
TorList=/var/tmp/torlist.txt

# cURL fetches Tor Relay list from https://check.torproject.org/exit-addresses
# grep identifies and extracts valid IP addresses from the list

curl -k https://check.torproject.org/exit-addresses | grep -E -o
'(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?
[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]
|2[0-4][0-9]|[01]?[0-9][0-9]?)' > $TorList

#Remove old Feed information before uploading new list
curl -k -v -XDELETE -H "Authorization: Bearer $APPToken" -F server='*'
https://threat-api.sky.junipersecurity.net/v1/cloudfeeds/blacklist/param/ip/${FeedName}

# Wait for 5 seconds before uploading new list
sleep 5

#Upload List to SkyATP as Feed Tor_Exit_Nodes
curl -k -v -XPOST -H "Authorization: Bearer $APPToken" -F file=@${TorList}
https://threat-api.sky.junipersecurity.net/v1/cloudfeeds/blacklist/file/ip/${FeedName}

# Cleanup
rm $TorList

# Exit
```

Once the script has been run successfully, we can see that the latest Tor Nodes are being blocked during an ICMP request below (**feed-name=Tor_Exit_Nodes**)

```
<14>1 2016-10-17T15:18:11.618Z SRX-1500 RT_SECINTEL - SECINTEL_ACTION_LOG
[junos@x.x.x.x.x.137 category="secintel" sub-category="Blacklist" action="BLOCK"
 action-detail="DROP" http-host="N/A" threat-severity="0"
source-address="5.196.121.161" source-port="1" destination-address="x.x.0.10"
destination-port="24039" protocol-id="1" application="N/A" nested-application="N/A"
 feed-name="Tor_Exit_Nodes" policy-name="cc_policy" profile-name="Blacklist"
username="N/A" roles="N/A" session-id-32="572564" source-zone-name="Outside"
destination-zone-name="DMZ"] category=secintel sub-category=Blacklist action=BLOCK
 action-detail=DROP http-host=N/A threat-severity=0 source-address=x.x.0.110
```

```
source-port=1 destination-address=x.x.x.161 destination-port=24039 protocol-id=1
 application=N/A nested-application=N/A feed-name=Tor_Exit_Nodes
policy-name=cc_policy profile-name=Blacklist username=N/A roles=N/A
session-id-32=572564 source-zone-name=Outside destination-zone-name=DMZ
```

SRX Series Update Intervals for Cloud Feeds

The following table provides the update intervals for each feed type. Note that when the SRX Series device makes requests for new and updated feed content, if there is no new content, no updates are downloaded at that time.

Table 2: Feed Update Intervals

Category	Feeds	SRX Update Intervals (in seconds)
Command and Control	Juniper Feeds	1,800
	Integrated Feeds	1,800
	Customer Feeds	1,800
GeoIP	geoip_country	435,600
Whitelist	Customer Feeds	3,600
Blacklist	Customer Feeds	3,600
Infected Hosts	Infected Hosts	60
IPFilter	Customer Feeds	1,800
	Office 365	1,800

Related Documentation

- Threat Intelligence Open API Reference Guide
- Juniper Sky ATP Open API Reference Guide

Modified: 2018-06-13