Secure Network Analytics Understanding External Connections Guide

Contents

Introduction

External Connections

Additional Information

Cisco Secured Service Exchange (SSE)

Region and Hosts

Direct Software Downloads (Beta)

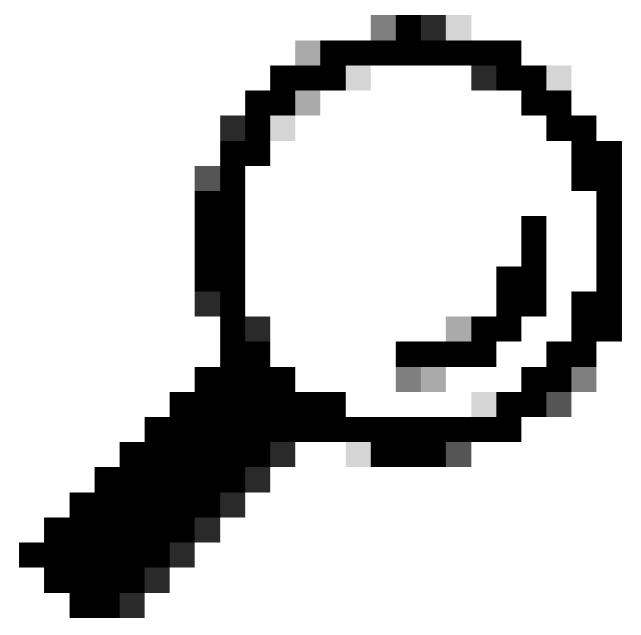
MITRE ATT&CK® Framework

Threat Feed

Contacting Support

Introduction

Use this guide to review external connections that are required for certain Secure Network Analytics features to operate expeditiously. These external connections can be domains or endpoints. Domains are names used for identifying resources on the internet, usually websites or services; and endpoints are actual devices or nodes that communicate across a network. Since the focus for this guide is web services, these will be shown as URLs. The table lists the external connection URLs in alphabetical order.



Tip: The table lists the external connection URLs in alphabetical order.

External Connections

External Connection URL	Purpose
https://analytics.int.obsrvbl.com	Used by Secure Network Analytics for telemetry data exchange with Secure Cloud Analytics services.
https://api.apj.sse.itd.cisco.com	Required by Cisco for data transit to Amazon Web Services (AWS)

	for the Asia Pacific, Japan, and China (APJC) region. Used when forwarding alerts
	to Cisco XDR and also for customer service metrics.
https://api.eu.sse.itd.cisco.com	Required by Cisco for data transit to Amazon Web Services (AWS) for the Europe (EU) region. Used when forwarding alerts to Cisco XDR and also for customer service metrics.
https://api-sse.cisco.com	Required by Cisco for data transit to Amazon Web Services (AWS) for the United States (US) region. Used when forwarding alerts to Cisco XDR and also for customer service/success metrics.
https://apix.cisco.com	Used by Secure Network Analytics for the Direct Software Downloads feature.
https://dex.sse.itd.cisco.com	Required for the sending and collection of customer success metrics
https://est.sco.cisco.com	Required for the sending and collection of customer success metrics
https://eventing-ingest.sse.itd.cisco.com	Required for the sending and collection of customer success metrics
https://feodotracker.abuse.ch/downloads/ipblocklist.txt	Required by Threat Feed, which is used for Secure

	NT-4
	Network Analytics
	alerts and
	observations, when
	Analytics is
	enabled.
	Used by Secure
	Network Analytics
https://id.cisco.com	for the Direct
	Software
	Downloads feature.
	Required by Threat
	Feed, which is
	used for Secure
https://intelligence.sourcefire.com/auto-update/auto-	Network Analytics
dl.cgi/00:00:00:00:00/Download/files/ip-filter.gz	alerts and
whogs core are are are are are are are are are a	observations, when
	Analytics is
	enabled.
	Required by Threat
	Feed, which is
	· /
https://intalligenee.sourcefire.com/outs.undata/outs	used for Secure
https://intelligence.sourcefire.com/auto-update/auto-	Network Analytics
dl.cgi/00:00:00:00:00/Download/files/url-filter.gz	alerts and
	observations, when
	Analytics is
	enabled.
	Required by
	Secure Network
	Analytics Threat
	Intelligence Feed,
	which is used for
	Secure Network
https://lancope.flexnetoperations.com/control/lncp/LancopeDownload	Analytics alarms
	and security
	events. This
	requires the Secure
	Network Analytics
	Threat Intelligence
	Feed license.
	Required for the
	sending and
https://mx*.sse.itd.cisco.com	collection of
1	customer success
	metrics
	Allows for
	accessing MITRE
https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ic	information for
attack.json	alerts when
mundarijo Ott	Analytics is
	enabled.
	Allows for
https://row.githubusgraantant.com/mitra/ati/mostan/mahila	
https://raw.githubusercontent.com/mitre/cti/master/mobile-	accessing MITRE information for
attack/mobile-attack.json	
	alerts when

	Analytics is
	enabled.
	Allows for
httms://www.cithyhysomontout.com/withy/oti/wootou/outowsiss	accessing MITRE
https://raw.githubusercontent.com/mitre/cti/master/enterprise-	information for
attack/enterprise-attack.json	alerts when
	Analytics is
	enabled.
	Required Threat
	Feed, which is
	used for Secure
https://s3.amazonaws.com/onconfig/global-blacklist	Network Analytics
intps://so.amazonaws.com/oncomig/groodi/onackiist	alerts and
	observations, when
	Analytics is
	enabled.
	Required by Cisco
	for data transit to
	Amazon Web
	Services (AWS)
	for the Asia
	Pacific, Japan, and
https://sensor.anz-prod.obsrvbl.com	China (APJC)
	region. Used when
	forwarding alerts
	to Cisco XDR and
	also for customer
	service metrics.
	Required by Cisco
	for data transit to
	Amazon Web
	Services (AWS)
	for the Europe
https://sensor.eu-prod.obsrvbl.com	(EU) region. Used
intps://sensor.eu-prod.obsrvor.com	when forwarding
	alerts to Cisco
	XDR and also for
	customer service
	metrics.
	Required by Cisco
	for data transit to
	Amazon Web
	Services (AWS)
1	for the United
https://sensor.ext.obsrvbl.com	States (US) region.
	Used when
	forwarding alerts
	to Cisco XDR and
	also for customer
	service metrics.
	Used to access
	Cisco Smart
smartreceiver.cisco.com	Software
	Licensing. Refer to

Licensing Guide for details. Alternativ offline licensing is available, if preferred. Refer to the Release Notes for details. Used by Secure Network Analytic for the Direct Software Downloads featur Required for the		the Smart
for details. Alternative offline licensing is available, if preferred. Refer to the Release Notes for details. Used by Secure Network Analytic for the Direct Software Downloads featur Required for the		
details. Alternative offline licensing is available, if preferred. Refer to the Release Notes for details. Used by Secure Network Analytic for the Direct Software Downloads featur Required for the		
offline licensing is available, if preferred. Refer to the Release Notes for details. Used by Secure Network Analytic for the Direct Software Downloads featur Required for the		
available, if preferred. Refer to the Release Notes for details. Used by Secure Network Analytic for the Direct Software Downloads featur Required for the		details. Alternative
preferred. Refer to the Release Notes for details. Used by Secure Network Analytic for the Direct Software Downloads featur Required for the		offline licensing is
the Release Notes for details. Used by Secure Network Analytic for the Direct Software Downloads featur Required for the		available, if
for details. Used by Secure Network Analytic for the Direct Software Downloads featur Required for the		preferred. Refer to
Used by Secure Network Analytic for the Direct Software Downloads featur Required for the		the Release Notes
Network Analytic for the Direct Software Downloads featur Required for the		for details.
https://software.cisco.com for the Direct Software Downloads featur Required for the	https://software.cisco.com	Used by Secure
Software Downloads featur Required for the		Network Analytics
Downloads featur Required for the		for the Direct
Required for the		Software
		Downloads feature.
l	https://www.cisco.com	Required for the
Cisco domain,		Cisco domain,
which is used for		which is used for
https://www.cisco.com Smart Licensing,		Smart Licensing,
cloud proxy, and		cloud proxy, and
firewall connection		firewall connection
		tests.

Additional Information

To further assess how and why specific domain and endpoint connections are used, refer to the following topics:

- Cisco Secured Service Exchange (SSE)
- Direct Software Downloads (Beta)
- MITRE ATT&CK® Framework
- Threat Feed

Cisco Secured Service Exchange (SSE)

SSE endpoints are used for data transit to Amazon Web Services (AWS), by Cisco for customer service metrics, and also used when forwarding alerts to Cisco XDR. These vary based on Region and Hosts. These endpoints are discovered dynamically using a Service Discovery mechanism provided by the SSE Connector. When publishing detections to Cisco XDR, Secure Network Analytics attempts to discover a service titled "xdr-data-platform" and its API endpoint "Events."

Region and Hosts

Depending on the region in production environments, the hosts are as follows.

US:

- https://api-sse.cisco.com
- https://sensor.ext.obsrvbl.com

EU:

- https://api.eu.sse.itd.cisco.com
- https://sensor.eu-prod.obsrvbl.com

APJC:

- https://api.apj.sse.itd.cisco.com
- https://sensor.anz-prod.obsrvbl.com

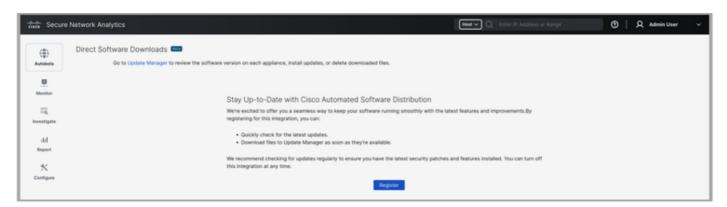
Direct Software Downloads (Beta)

The following connections are used by the Direct Software Downloads feature:

- https://apix.cisco.com
- https://software.cisco.com
- https://id.cisco.com

To use this new feature to download software and patch update files directly to your Update Manager, make sure you've registered using your cisco.com user ID (CCOID).

- 1. Log in to the Manager.
- 2. From the main menu, choose **Configure > Global > Central Management**.
- 3. Click the **Update Manager** tab.
- 4. Click the **Direct Software Downloads** link to open the registration page.
- 5. Click the **Register** button to begin the registration process.



- 6. Click the link that is provided.
- 7. You will be taken to the Activate Your Device page. Click Next to continue.
- 8. Log in with your cisco.com user ID (CCOID).
- 9. You will receive a "Device Activated" message once your activation is complete.
- 10. Go back to the Direct Software Downloads page on your Manager and click Continue.
- 11. Click the links for the EULA and K9 agreements to read and accept the terms. Once the terms are accepted, click **Continue**.

For more information about Direct Software Downloads, contact Cisco Support

MITRE ATT&CK® Framework

The MITRE ATT&CK® Framework is a publicly available knowledge base of adversary tactics and techniques based on real-world observations. When you've enabled Analytics within Secure Network Analytics, MITRE tactics and techniques assist with cybersecurity threat intelligence, detection, and

response.



To make sure Analytics is enabled, choose **Configure > Detection > Analytics** from the main menu, then click *Analytics On Analytics On*

The following connections allow Secure Network Analytics to access MITRE information for alerts:

- https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
- https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobileattack.json
- https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterpriseattack.json

Threat Feed

The Cisco Secure Network Analytics Threat Feed (formerly Stealthwatch Threat Intelligence Feed) provides data from the global Threat Feed about threats to your network. The feed updates frequently and includes IP addresses, port numbers, protocols, host names, and URLs known to be used for malicious activity. The following host groups are included in the feed: command-and-control servers, bogons, and Tors.

To enable Threat Feed in Central Management, follow the instructions in the Help.

- 1. Log in to your primary Manager.
- 2. Select Configure > Global > Central Management.
- 3. Click the (**Help**) icon. Select **Help**.
- 4. Select **Appliance Configuration > Threat Feed**.



Please note that you will configure the DNS server and firewall as part of the instructions. Also, if you have a failover configuration, you need to enable Threat Feed on your primary Manager and secondary Manager.

For more information about Threat Feed, refer to the **System Configuration Guide**.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html