Secure Network Analytics 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 are shown as URLs. 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)

External Connection URL	Purpose
	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 Network Analytics alerts and observations, when Analytics is enabled.
https://id.cisco.com	Used by Secure Network Analytics for the Direct Software Downloads feature.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/ip-filter.gz	Required by Threat Feed, which is used for Secure Network Analytics alerts and observations, when Analytics is enabled.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/url-filter.gz	Required by Threat Feed, which is used for Secure Network Analytics alerts and observations, when Analytics is enabled.
https://lancope.flexnetoperations.com/control/lncp/LancopeDownload	Required by Secure Network Analytics Threat Intelligence Feed, which is used for Secure Network Analytics alarms and security events. This requires the Secure Network Analytics Threat Intelligence Feed license.
https://mx*.sse.itd.cisco.com	Required for the sending and collection of customer success metrics
https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json	Allows for accessing MITRE information for alerts when Analytics is enabled.
https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json	Allows for accessing MITRE information for alerts when Analytics is enabled.
https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json	Allows access to MITRE information for alerts when Analytics is enabled.
https://brlcbwaicj.execute-api.us-east-1.amazonaws.com/test/get-doh-intel	Required Threat Feed, which is used for Secure Network

External Connection URL	Purpose
	Analytics alerts and observations, when Analytics is enabled.
https://s3.amazonaws.com/onconfig/global-blacklist	Required Threat Feed, which is used for Secure Network Analytics alerts and observations, when Analytics is enabled.
https://sensor.anz-prod.obsrvbl.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://sensor.eu-prod.obsrvbl.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://sensor.ext.obsrvbl.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 metrics.
https://smartreceiver.cisco.com	Used to access Cisco Smart Software Licensing. Refer to the Smart Licensing Guide for details. Alternative offline licensing is available, if preferred. Refer to the Release Notes for details.
https://software.cisco.com	Used by Secure Network Analytics for the Direct Software Downloads feature.
https://softwarecloud.cisco.com	Used by Secure Network Analytics for the Direct Software Downloads feature.
https://www.cisco.com	Required for the Cisco domain, which is used for Smart Licensing, cloud proxy, and firewall connection tests.

Additional Information

To further assess how and why specific domain and endpoint connections are used, see:

- 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 your service metrics, and when forwarding alerts to Cisco XDR. They vary based on Region and Hosts. 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, these are the hosts:

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

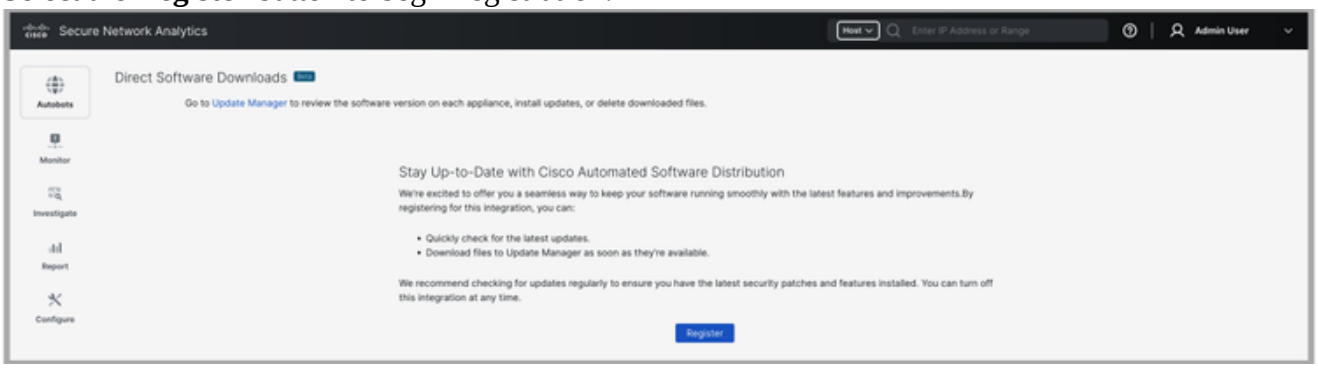
Direct Software Downloads (Beta)

The Direct Software Downloads feature uses these connections:

- 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, select **Configure** > **Global** > **Central Management**.
3. Select the **Update Manager** tab.
4. Select the **Direct Software Downloads** link to open the registration page.
5. Select the **Register** button to begin registration.

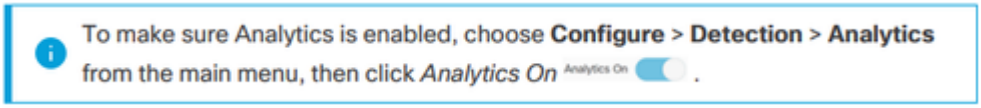


6. Click the link provided.
7. At the Activate Your Device page, select **Next**.
8. Log in with your cisco.com user ID (CCOID).
9. A "Device Activated" message appears once your activation is complete.
10. Go back to the Direct Software Downloads page on your Manager and select **Continue**.
11. Select the links for the EULA and K9 agreements to read and accept the terms. Once the terms are accepted, select **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.



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

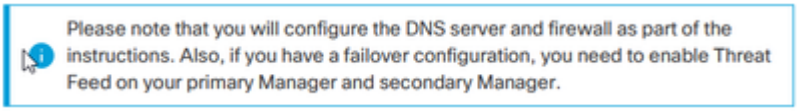
Threat Feed

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. Select the **(Help) icon** and then **Help**.
4. Select **Appliance Configuration** > **Threat Feed**.



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

Contacting Support

For technical support:

- Contact your local Cisco Partner
- Contact Cisco Support
- Open a case at Cisco Support
- Call 1-800-553-2447 (U.S.)
- Find worldwide support numbers at Cisco Worldwide Support Contacts