



Cisco Secure Network Analytics

Send On-Premises Flows from Cisco Telemetry Broker or Secure Network Analytics to Cisco XDR Analytics Configuration Guide 7.5.1



Table of Contents

| | |
|---|-----------|
| Overview | 3 |
| Supported Flow Data Types | 3 |
| Cisco Telemetry Broker Configuration | 4 |
| Prerequisites | 4 |
| Configure Cisco Telemetry Broker | 4 |
| Flow Collector Configuration | 6 |
| Prerequisites | 6 |
| Resource Requirements | 6 |
| Enable Sending Flows to XDR Analytics | 6 |
| Disable Sending Flows to XDR Analytics | 7 |
| Configure Proxy | 7 |
| Verification | 9 |
| Contacting Support | 11 |
| Change History | 12 |

Overview

This guide explains how to configure on-premises flow data to be sent from Cisco Telemetry Broker (CTB) or Secure Network Analytics (formerly Stealthwatch) to Cisco XDR Analytics (formerly Stealthwatch Cloud).



We recommend using Cisco Telemetry Broker to send on-premise flow data to XDR Analytics. Alternatively, you can configure the Flow Collector to send flow data directly to Cisco XDR Analytics. For more information, review the [Flow Collector Resource Requirements](#).

Supported Flow Data Types

The following types of flow data are sent from Secure Network Analytics to XDR Analytics using Cisco Telemetry Broker or the Flow Collector:

- IPFIX packets
- NetFlow v5 (Cisco Telemetry Broker v1.3 or later)
- NetFlow v9 (Cisco Telemetry Broker v1.3 or later)



Network Visibility Module (NVM) data is not supported in XDR Analytics. If your Secure Network Analytics deployment ingests NVM data, we suggest using a dedicated flow-based telemetry Flow Collector to send on-premises flow data and using a separate Flow Collector to ingest NVM data.

Cisco Telemetry Broker Configuration

Use the following instructions to configure your Cisco Telemetry Broker to send on-premise flow data to XDR Analytics. We recommend using this method for environments with over 50,000 Flows per Second (FPS).

Prerequisites

- XDR Analytics account
- Cisco Telemetry Broker v1.2 or later



To deploy a Cisco Telemetry Broker, follow the instructions in the [Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide](#).



Configure Cisco Telemetry Broker

1. Log in to your XDR Analytics web portal.
2. Click **Settings > Sensors**.
3. Scroll to the bottom of the page and save the Service key and Service host information.

Service key: [REDACTED]

Service host: `https://[REDACTED].obsrvbl.com`

4. Log in to Cisco Telemetry Broker.
5. In the upper right corner of the page, click **Add Destination > SCA Destination**.
6. Enter a destination **Name**.
7. Enter the **SCA Service Key**. Make sure that you paste the entire key.
8. Enter the **SCA Host URL**. Make sure that you paste the entire URL.
9. Click **Save**.
10. Go back to the Sensors page in the XDR Analytics portal. You should see the Telemetry Broker hostname and information included in the sensors list.

 Settings ▾
Hostname: ctb
Heartbeat Received: ● 2022-07-31 12:40:30 UTC
Heartbeat Sent: 2022-07-31 12:40:33 UTC
Last Flow Record: ● 2022-06-22 10:47:42 UTC
[all sensor details >](#)



For more information on configuring Destinations, refer to the [Cisco Telemetry Broker User Guide](#).

Flow Collector Configuration

Use the following instructions to configure your Flow Collector to send on-premises flow data to XDR Analytics.



If you have configured Cisco Telemetry Broker to send on-premises flow data, you do not need to configure your Flow Collector. You only need to export flow data to XDR Analytics once per area of the network.

Prerequisites

- XDR Analytics account
- Secure Network Analytics Flow Collector v7.5.1

Resource Requirements

If sending on-premises flow data directly from your Flow Collector to XDR Analytics, we recommend the Flow Collector has the following allocated resources:

| Flows per Second (FPS) | Required Reserved Memory | Required Reserved CPUs | Required Minimum Data Storage |
|------------------------|--------------------------|------------------------|-------------------------------|
| Up to 300k | 70 GB | 8 | 200 GB |



For environments with more than 300k FPS, we recommend configuring [Cisco Telemetry Broker](#) to send the on-premises flow data.

Enable Sending Flows to XDR Analytics

1. Log in to your XDR Analytics web portal.
2. Click **Settings > Sensors**.
3. Scroll to the bottom of the page and save the Service key and Service host information.

Service key:

Service host: `https://` `.obsrvbl.com`

4. Log in to your appliance console as **sysadmin**.
5. Select **Advanced**.
6. Select **Cloud: Send flows to Cisco XDR Analytics**.
7. Enter the Service Key and Service URL and click **OK**.
8. When prompted to confirm that you want to use these settings, click **Yes**.

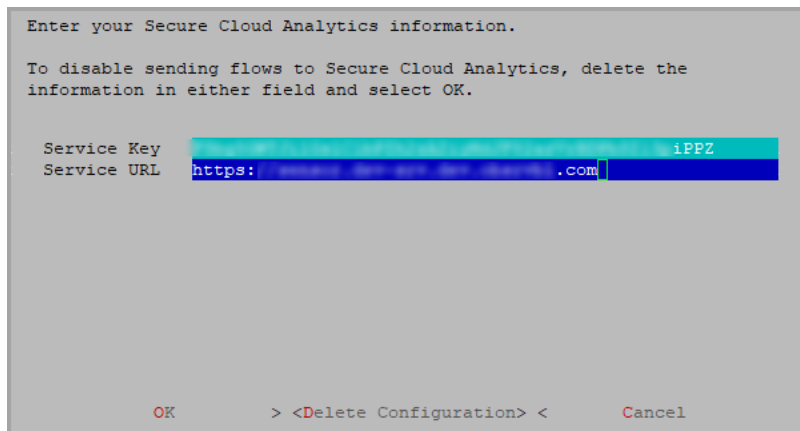
You will receive a confirmation message stating that you have successfully save your XDR Analytics configuration.

Disable Sending Flows to XDR Analytics

To disable sending flows to XDR Analytics, complete the following steps:

1. Log in to your appliance console as **sysadmin**.
2. Select **Advanced**.
3. Select **Cloud: Send flows to Cisco XDR Analytics**.

The following screen opens.





4. Click **Delete Configuration**.
5. Click **OK**.
6. When prompted to confirm that you want to disable sending flows to XDR Analytics, click **Yes**.

You will receive a confirmation message stating that you have successfully disabled sending flows to XDR Analytics.

Configure Proxy

If your Flow Collector does not have a direct connection to the internet, you will need to configure Internet Proxy to reach XDR Analytics.


1. Log in to your Manager.
2. From the navigation menu, click **Configure > Global > Central Management**.
3. Click the **⋮ (Ellipsis)** icon for your Flow Collector, then click **Edit Appliance Configuration**.
4. Click the **Network Service** tab, scroll to the Internet Proxy section.
5. Enter the IP address and Port information.

 For instructions on how to configure Internet Proxy, click the  **(User)** icon, then click **Help > Internet Proxy**. The IP Address, Port, and Proxy Login Credentials are specific to your network. Contact your Network Administrator for assistance.


Appliance Configuration - Flow Collector

Appliance **Network Services** General

Internet Proxy **Modification Requires Reboot**

 Confirm your DNS server is configured.

Proxy Setup

Enable 

IP Address *

Port *

Proxy Login Credentials (if applicable)

User Name

Password

Authentication Type

basic

ntlm

Domain

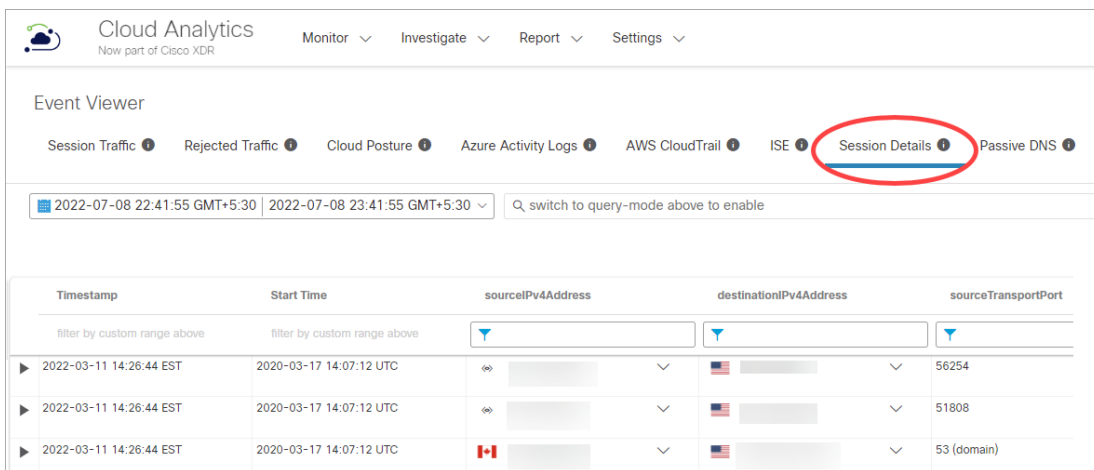
6. Click **Apply Settings**.
7. Follow the on-screen prompts. The appliance reboots automatically.

Verification

Use the following instructions to verify XDR Analytics is receiving on-premises flow data.

i After configuration, you should be able to see flow records from Cisco Telemetry Broker or the Flow Collector in XDR Analytics within 30 minutes. If you do not, please contact [Cisco Support](#).

1. Log in to your XDR Analytics web portal.
2. Go to **Investigate > Event Viewer**.
3. Click the **Session Details** tab.



The screenshot shows the Cloud Analytics web portal interface. The top navigation bar includes 'Monitor', 'Investigate', 'Report', and 'Settings'. The main content area is titled 'Event Viewer' and contains several tabs: 'Session Traffic', 'Rejected Traffic', 'Cloud Posture', 'Azure Activity Logs', 'AWS CloudTrail', 'ISE', 'Session Details' (highlighted with a red circle), and 'Passive DNS'. Below the tabs, there are two date range selectors and a search bar. The main data area is a table with the following columns: 'Timestamp', 'Start Time', 'sourceIPv4Address', 'destinationIPv4Address', and 'sourceTransportPort'. The table contains three rows of data, each with a play button icon on the left.

| Timestamp | Start Time | sourceIPv4Address | destinationIPv4Address | sourceTransportPort |
|---------------------------|-------------------------|-------------------|------------------------|---------------------|
| ▶ 2022-03-11 14:26:44 EST | 2020-03-17 14:07:12 UTC | ∞ [redacted] ▼ | 🇺🇸 [redacted] ▼ | 56254 |
| ▶ 2022-03-11 14:26:44 EST | 2020-03-17 14:07:12 UTC | ∞ [redacted] ▼ | 🇺🇸 [redacted] ▼ | 51808 |
| ▶ 2022-03-11 14:26:44 EST | 2020-03-17 14:07:12 UTC | 🇨🇦 [redacted] ▼ | 🇺🇸 [redacted] ▼ | 53 (domain) |

You will see the flow records from the Cisco Telemetry Broker or the Flow Collector.

Copyright Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



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>
- To open a case by email: tac@cisco.com
- 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>

Change History

| Document Version | Published Date | Description |
|------------------|-----------------|------------------|
| 1_0 | August 16, 2024 | Initial version. |