



# Cisco Telemetry Broker

User Guide 2.1.3



---

# Table of Contents

<b>Introduction</b> .....	<b>8</b>
Audience .....	8
Common Terms .....	8
Configure Accessibility Features .....	9
Common Abbreviations .....	9
Alerts .....	10
<b>Overview</b> .....	<b>11</b>
Access the Overview Page .....	11
View the Following Components .....	11
Inputs .....	11
Destinations .....	11
Broker Nodes .....	12
Alerts .....	12
CPU .....	13
Licensing .....	14
Telemetry Flows .....	14
Metrics .....	14
<b>Data Flow</b> .....	<b>15</b>
How to Find This Page .....	15
View Snapshot Information .....	15
View Data Flows .....	16
Click vs. Hover .....	16
Notification and Status Indicators .....	17
Filter Your Search .....	18
Filter .....	18
Clear Filters .....	19
Search .....	19
Import UDP Director Configuration .....	19

---

Inputs .....	20
Add an Input .....	20
Edit an Input .....	20
Delete an Input .....	21
Destinations .....	21
Add a Destination .....	21
Edit a Destination .....	21
Delete a Destination .....	21
Connections .....	22
Create a Connection .....	22
Edit a Connection .....	22
Delete a Connection .....	23
Broker Nodes and Clusters .....	23
Activate Broker Nodes and Clusters for an Input .....	23
Edit Assigned Broker nodes and Clusters .....	23
<b>Destinations .....</b>	<b>24</b>
How to Find This Page .....	24
Import UDP Director Configuration .....	25
Filter Your Search .....	25
Filter .....	25
Clear Filters .....	25
Search .....	26
Sort Columns .....	26
Add a Destination .....	26
Add a UDP Destination .....	26
Reachability Check .....	26
Add a Secure Cloud Analytics (SCA) Destination .....	27
Locate the key and the URL .....	27
Add the SCA destination .....	27
Edit a Destination .....	28

---

Remove a Destination .....	28
View Details of a Destination .....	28
Destination Details .....	28
General Information .....	28
Notifications .....	29
Sent Rate .....	29
Edit a Destination .....	29
Remove a Destination .....	29
Connected Inputs/Exporters .....	30
Information Included in the Table .....	30
Metrics: Sent Rate .....	31
<b>Inputs .....</b>	<b>32</b>
How to Find This Page .....	33
Filter Your Search .....	33
Filter .....	33
Clear Filters .....	33
Search .....	33
Sort Columns .....	34
Import UDP Director Configuration .....	34
Add an Input .....	34
Disable Exporters Tracking .....	35
Edit an Input .....	36
Remove an Input .....	36
View Details of an Input .....	36
Broker Nodes and Clusters .....	36
Activate Broker Nodes and Clusters .....	36
Edit Assigned Broker Nodes and Clusters .....	37
Input Details .....	37
General Information .....	37
Notifications .....	38

---

Received Rate .....	38
More Details .....	38
Edit an Input .....	38
Remove an Input .....	38
Connected Destinations .....	39
Create a Connection .....	39
Edit a Connection .....	39
Remove a Connection .....	40
Metrics .....	40
Exporters .....	40
Search .....	41
Filter .....	41
Disable Exporters Tracking .....	41
Add a Flow Generator Input .....	42
<b>Broker Nodes .....</b>	<b>43</b>
Add a Cluster .....	43
View Details of a Broker Node .....	43
Broker Node Details .....	43
General Section .....	43
Telemetry Interface .....	44
Monitor Interface .....	44
Edit a Broker Node .....	44
Remove a Broker Node .....	45
Metrics .....	45
Received Rate table .....	45
Sent Rate table .....	46
1-Minute Load Average table .....	47
Memory Usage table .....	47
Disk Storage table .....	47
<b>High Availability Clusters .....</b>	<b>48</b>

---

Cluster Tasks .....	49
View Cluster Details .....	49
Add a Cluster .....	49
Modify a Cluster's Configuration .....	49
Remove a Cluster .....	50
<b>Manager Node .....</b>	<b>51</b>
How to Find This Page .....	51
1-Minute Load Average table .....	51
Memory Usage table .....	51
Disk Storage table .....	51
<b>Application Settings .....</b>	<b>53</b>
General .....	53
Configure Inactivity Interval .....	53
Configure HTTPS Proxy .....	53
Software Update .....	53
Upgrade Your Cisco Telemetry Broker Deployment .....	54
Download the Update File .....	54
Upload the Update File .....	54
Smart Licensing .....	55
User Management .....	55
Add a User .....	55
Edit a User .....	56
Remove a User .....	56
Change a User's Password .....	56
TLS Certificate .....	56
Upload TLS Certificate .....	56
Re-register Broker Nodes .....	57
Syslog Notifications .....	57
Configure the Syslog Server .....	57
Enable the Syslog Server to Receive Notifications .....	58

---

Send a Test Syslog Notification .....	58
Severity and Facility Values .....	58
Email Notifications .....	58
Configure the SMTP Server .....	59
Enable a User to Receive Email Notifications .....	59
Send a Test Email Notification .....	59
<b>Profile Settings .....</b>	<b>60</b>
Edit Your Personal Information .....	60
Change Your Password .....	60
<b>Expand Cisco Telemetry Broker Manager and Broker Node Disk Size .....</b>	<b>61</b>
1. Back Up the Partition Table Information .....	61
2. Delete All Existing VM Snapshots for the Appliance .....	61
3. Increase the Disk Size of the Appliance .....	62
4. Run ctb-part-resize.sh Script .....	62
5. Verify that Space has been Allocated .....	63
<b>Shut Down or Reboot Cisco Telemetry Broker .....</b>	<b>64</b>
<b>Appendix A: Supported IPFIX Fields for Cisco Telemetry Broker .....</b>	<b>65</b>
<b>Appendix B: Supported Alerts .....</b>	<b>94</b>
<b>Appendix C: Import UDP Director Configuration .....</b>	<b>95</b>
Export Your UDP Director Configuration .....	95
Export Your UDP Director Configuration From a Manager .....	95
Import Your UDP Director Configuration into Cisco Telemetry Broker .....	95
<b>Contact Support .....</b>	<b>96</b>
<b>Change History .....</b>	<b>97</b>

# Introduction

This guide provides a reference for the Cisco Telemetry Broker Manager web interface.

Cisco Telemetry Broker (at times referred to as CTB in this document) enables you to ingest network telemetry from many inputs, transform the telemetry format, and forward that telemetry to one or multiple destinations.

## Audience

This guide is designed for the person responsible for maintaining network telemetry flow and monitoring network telemetry.

## Common Terms

The following terms appear in this guide:

Abbreviation	Description
Destinations	Locations to which Cisco Telemetry Broker forwards telemetry. Cisco Telemetry Broker supports multiple types of destinations.
Exporters	Devices on a customer's network that forward traffic to an Input on the Cisco Telemetry Broker. Exporters are typically defined by an IP address.
Inputs	Ways in which Cisco Telemetry Broker collects or receives telemetry from a customer network. Cisco Telemetry Broker supports multiple types of inputs.
Connections	User-defined logic that tells Cisco Telemetry Broker how to forward telemetry from a single input to a single destination.
Telemetry	Any type of data that the Customer produces that is useful for analytical purposes. Examples include UDP packets, IPFIX, syslog, and JSON.



If you are currently using UDP Director, note that you can import your existing forwarding rules as an XML file and import it into Cisco Telemetry Broker. You need to make sure you do this before you add any destinations. For more details, see [Import UDP Director Configuration](#).



## Configure Accessibility Features

In order to have access to configure available website accessibility features, you must use Chrome as your browser when using the Cisco Telemetry Broker Manager web interface. Following are examples of some accessibility features you won't have the ability to configure if you use a browser other than Chrome. (This list is not comprehensive.)

The ability to do the following:

- Highlight each item on a web page
- Show color in compact tab bar
- Specify to never use certain font sizes

## Common Abbreviations

The following abbreviations appear in this guide:

<b>Abbreviation</b>	<b>Description</b>
DNS	Domain Name Server
GB	Gigabyte
HTTPS	Hypertext Transfer Protocol (Secure)
ISE	Identity Services Engine
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol
SSH	Secure Shell
TAP	Test Access Port
UDPD	UDP Director
UPS	Uninterruptible Power Supply
URL	Universal Resource Locator

Abbreviation	Description
VLAN	Virtual Local Area Network
VM	Virtual Machine

## Alerts

When one or more alerts exist for an entity (any configured destination, input, or broker node), a status indicator is displayed next to the associated main menu heading, along with a number.



This number reflects the number of entities in that entity category that contain an alert.

When an entity has multiple issues (for example, a destination simultaneously being unreachable and not having any connections, or an input not have any destinations and also being inactive), Cisco Telemetry Broker considers this one issue. It does not calculate the number of issues based on the individual number of existing issues. So, for example, if an entity has 5 different issues, Cisco Telemetry Broker considers this 1 issue, not 5 issues.

---

# Overview

This page provides a snapshot of the configuration settings, system health, main metrics, and licensing information for your Cisco Telemetry Broker system.

## Access the Overview Page

From the Cisco Telemetry Broker main menu, choose **Overview**, or click the Cisco logo (in the upper left corner of the page).

## View the Following Components

### Inputs

This component displays telemetry for the last 24 hours for the following information:

- The number of inputs that have been configured in Cisco Telemetry Broker.
- The amount of telemetry received from all inputs.
- The average value is calculated from the last 30 days of telemetry.
- The number of inputs for which no connection has been configured. This number is represented by the number in the **No Destination** field.
- Each segment on the doughnut chart displays the amount of telemetry received from each input. When you hover your cursor over a segment of this chart, you can view the following information:
  - the input name
  - the amount of telemetry received from this specific input for the last 24 hours

### Destinations

This component displays telemetry for the last 24 hours for the following information:

- The number of destinations that have been configured in Cisco Telemetry Broker.
- The amount of telemetry sent to all destinations.
- The average daily rate of telemetry sent to all destinations. The average value is calculated from the last 30 days of telemetry.
- The number of destinations not accepting telemetry that is being sent to them (represented by the number in the Unreachable field). When you click this number,

the Destinations page opens. The list of destinations that are unreachable are listed here.

- Each segment on the doughnut chart displays the amount of telemetry sent to each destination. When you hover your cursor over a segment of this chart, you can view the following information:
  - the destination name
  - the amount of telemetry sent to this specific destination for the last 24 hours

## Broker Nodes

This section is grouped by cluster, under the associated cluster name. If no high availability clusters exist, all broker nodes are grouped under the "No Cluster" subheading.

- Each arc shows the percentage of the broker node's received rate against the node's theoretical capacity. The arc is marked with the applicable color. Refer to the following table for an explanation of an arc's color.

Color	Definition
Red (Critical)	The percentage of capacity reached for the broker node is 100%.
Orange (Warning)	The percentage of capacity reached for the broker node is from 80% to 99.99%.
Blue (Informational)	The percentage of capacity reached for the broker node is < (less than) 80%.

- To access a broker node's page, click the node's name.
- If a broker node has any alerts, they are displayed underneath the node. They are marked by a white X on a red background with a short explanation.

## Alerts

The Alerts component lists the last 10 alerts that have either occurred and are still active, or that have been resolved. Alerts in red are still active, and alerts in gray have been resolved. The list begins with the newest alert at the top and ends with the oldest alert at the bottom. To view additional alerts, click the **See more...** link at the bottom of the list.

- The number of unresolved alerts and the number of all alerts in Cisco Telemetry Broker is displayed in the upper right corner of this component.
- By default, the list of all the unresolved alerts is displayed.
- To see a list of filter options, use the **Most Recent on Top** drop-down list.
- To see a list of all the alerts, click the **All filter option** in the top right corner of this component.
- Under each alert is information about the associated entity (for example, broker node or destination) as well as the time the alert occurred.
- When an alert is no longer valid (has been resolved), the alert is
  - dimmed
  - marked with a check mark, and
  - noted with the time it was resolved.
- When you click a link that appears under each alert name, either the associated Broker Node page or the Destinations page opens, depending on the alert type.

## CPU

For both the Manager node and each broker node, this component shows telemetry for the last 30 days for the following information:

- Number of CPUs available.
- Percentage used of the available CPUs (represented by the bar color).
- The 1-minute load average per the number of available CPUs for each broker node (to see this data, hover over the broker node name.)

Refer to the following table for an explanation of the color displayed on each bar.

Color	Definition
Red (Critical)	The percentage of maximum CPU load reached for the node is 100%.
Orange (Warning)	The percentage of maximum CPU load reached for the node is from 80% to 99.99%.
Blue (Informational)	The percentage of maximum CPU load reached for the node is < (less than) 80%.

---

## Licensing

This component displays telemetry for the last 14 days.

- The dotted blue line shows the average GB per day for the last 7 days. To see this number, hover your cursor over the dotted line. This number is the entitlement number sent to Smart Software Licensing for calculating license fees, and it will match the value displayed on the Telemetry Broker Smart Licensing page.
- Each bar in the chart represents a different day. The bar at the rightmost side of the chart represents the previous day and then proceeds to each prior day as you move to the left.
- To see the exact amount of GB received for a specific day, hover your cursor over the associated bar. The date associated with this bar is also displayed.
- If a product is not yet registered, a warning displays in the upper right corner showing how many days remain until the trial license expires.

## Telemetry Flows

This component displays telemetry for the last 24 hours.

- The different types of telemetry received by all inputs (represented by telemetry on the left side of the chart) and sent to all destinations (represented by telemetry on the right side).
- To show the exact value for a flow, hover your cursor over the flow to open its tooltip.
- For SCA destinations, the telemetry statistics displayed here represent uncompressed data sent to SCA. Therefore, these statistics may be disproportionate to the actual telemetry sent (represented in the Destinations component).

## Metrics

The tables in this component display the following data for the last 24 hours:

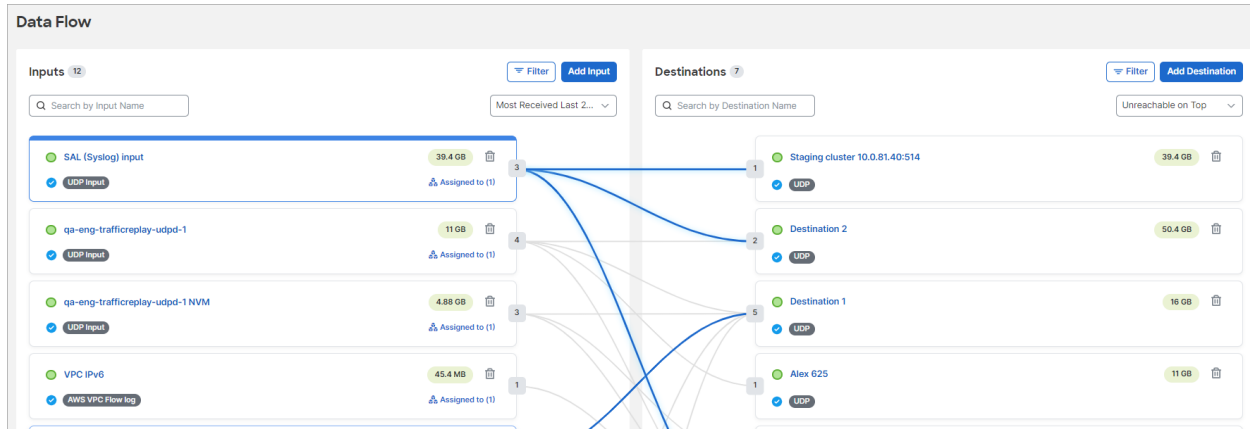
**Total Received Rate** The total amount of telemetry received from all inputs.

**Total Sent Rate** The total amount of telemetry sent to all destinations.

# Data Flow

Use this page to easily see which inputs and destinations are connected to each other. Keep in mind that multiple destinations can be connected to 1 input, and 1 destination can be connected to multiple inputs. On this page you can also view alerts, data flow information, and other details related to your configured inputs and destinations.

In the following image, the first input card as been selected.



## How to Find This Page

From the Cisco Telemetry Broker main menu, choose **Data Flow**.

## View Snapshot Information

- Input or destination name.
- Any applicable alert notifications.
- Input or destination type.
- The ✨ (**Highlight**) icon.
  - When you click this icon on an input card, all other input cards are hidden.
  - When you click this icon on a destination card, all other destination cards are hidden.
  - Click this icon a second time to return to the default view.
- The total data received (for inputs) or sent (for destinations) for the last 24 hours.
- The 🗑️ (**Remove**) icon.
- The number of inputs or destinations for a particular entity.



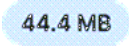
- (Input card) The number of destinations to which the input is connected, represented by the encircled number on the right edge of each card ( **12** ). If a **Plus** icon is displayed, this indicates that the input has no connected destinations.
- (Destination card) The number of inputs to which the destination is assigned, represented by the encircled number on the left edge of each card ( **12** ).
- (Input card only) The number of broker nodes and clusters to which the input is assigned. If none are assigned, the button says "Assign to." If any are assigned, the button says "Assigned to" and the number of assignments is displayed in parentheses.

## View Data Flows

The lines you see that connect various inputs to various destinations represent the connections that exist between those particular inputs and destinations. For information about adding connections, refer to the [Create a Connection](#) section.

You can view the data flows for any input or destination by clicking an input or destination card.

When you click a card, you can then click any of its connection lines to see the following information for that connection:

- The  (**Edit Connections**) icon . See [Edit a Connection](#).
- The  (**Remove**) icon. See [Delete a Connection](#).
- The  (**Sent Last 24**) icon. This number represents the amount of telemetry sent from the associated input to the associated destination for the last 24 hours.

### INSERT SCREENSHOT

Refer to the following table to learn what visual changes occur when you click vs. when you hover over a card. These visual changes enable you to more easily see the information related to the card you have chosen.

#### Click vs. Hover

When you ...	The
Hover over a	<ul style="list-style-type: none"> <li>• Border of the card turns blue.</li> </ul>








When you ...	The
card	<ul style="list-style-type: none"> <li>Data flow lines for that input or destination turn dark blue. All other lines on the Data Flow page remain light blue.</li> </ul>
Click a card	<ul style="list-style-type: none"> <li>Border of the card turns blue. The top border becomes thicker than the others.</li> <li>Data flow lines for that input or destination become bolded in blue. All other lines on the Data Flow page remain gray.</li> </ul>



To deselect a card, click it again or click anywhere outside the card (including clicking on another card).


## Notification and Status Indicators


To view the description for an existing notification or status indicator for a specific input or destination, hover your cursor over the associated icon. For a list of Cisco Telemetry Broker alerts, see [Appendix B: Supported Alerts](#).

Notification Icon	Description
<p>Notifications are messages that indicate that your system may not be working correctly or that you need to check an area on your system.</p>	
<p>Critical</p> 	<p>The only events that Cisco Telemetry Broker assigns this icon for on the Data Flow page is the following:</p> <p><b>Destinations Unreachable</b> This destination has sent a “destination unreachable” ICMP message.</p>
<p>Warning</p> 	<p>This icon is displayed for all other events that Cisco Telemetry Broker deems necessary for which to provide a warning.</p>
<p>No Notifications</p> 	<p>This icon indicates that the input or destination has no notifications associated with it.</p>
Status Indicator Icon	Description
<p>Status indicators inform you if inputs are receiving data that is within the configured Input &amp; Destination Inactivity Interval time frame, or if destinations are sending data that is within the configured Input &amp; Destination Inactivity Interval time frame.</p>	
<p>Active</p> 	<p>The associated input has received data at this moment or for the last time indicated by the configured Input &amp; Destination Inactivity Interval time frame (configured on the Settings &gt; General tab page).</p>
<p>Inactive</p> 	<p>The associated input is not receiving any data that is outside the configured Input &amp; Destination Inactivity Interval time frame.</p>

## Filter Your Search

### Filter

Use the  (**Filter**) icon to filter your search for inputs and destinations.

1. Click the  (**Filter**) icon in either the Inputs list or the Destinations list, depending on what you want to filter.

*Either the Filter Inputs or Filter Destinations dialog opens, within which are filter options you can choose.*

2. Choose as many filters as necessary, and when you are finished, click **Apply**. Note that in the Filter dialog for inputs, you also can filter by broker nodes and clusters.
3. (Conditional) If you want to reset the settings to what they originally were before you began to make changes, click **Reset**.



When you use one or more filters, all filters are ANDed together; therefore, all returned results must match the search criteria for all of the filters.

## Clear Filters

If you receive one or more results but do not see any for which you are searching, it could be that you have configured too many filters. In this instance, we recommend that you eliminate one filter at a time to see if any of your intended results show.

- If you want to clear an individual filter field or apply additional filters, click the Filter button (which contains the number of filters applied). When the Filter panel opens, make your changes and click **Apply**. Click **Reset** to remove all filter criteria.

## Search

In the Search field, type the name of the input or destination (depending on which list you are in) for which you are searching. As you start to type your entry, the field dynamically filters to display a list of entries that contains any of the characters you have entered.

Keep in mind that you can create multiple inputs with the same name, and the same applies to destination names. Port numbers among broker nodes can also be duplicated. So if you search for an input or destination for which there are more than one with the same name, or search for a port number that has been duplicated on two or more broker nodes, all matching entries will be displayed on the Data Flow page after your search has finished processing.

## Import UDP Director Configuration

From either the UDP Director, or the Manager that manages the UDP Director, you can export your current UDP Director destination and rule configuration as an XML file and import it into Cisco Telemetry Broker. For more details, see [Appendix C: Import UDP Director Configuration](#).





Once you have created your first destination, you no longer have the option to import a UDP Director configuration.



Importing a UDP Director configuration overwrites your current Cisco Telemetry Broker configuration, including all currently configured inputs, destinations, and rules.

## Inputs

On the right edge of each card, either the  (**Plus**) icon or the  (**Connected Destinations**) icon is displayed.

- If a **Plus** icon is displayed, this indicates that the input has no connected destinations.
- The **Connected Destination** icon displays the number of destinations to which the input is connected. When you hover over it, it changes to the **Plus** icon.

## Add an Input

To add an input, complete the following steps.

1. Click **Add Input** in the upper right corner of the Inputs list.

*The Add Input dialog opens.*

2. Choose the input type from the drop-down list and click **Next**.

*The second Add Input dialog opens.*

3. Configure all applicable fields and click **Add Input**.

*The Assignments dialog opens.*

4. (Optional) connect broker nodes or clusters to the input. Note that for some input types you will be able to add only a broker node.



If you don't connect broker nodes or clusters to the input at this step, you can do so later from the applicable input card on this page (click the **Assign to** button).

5. Click **Assign Nodes**.

*An input card for this input is now displayed in the Inputs list.*

## Edit an Input

1. Click the Input name within the applicable card.

*The Edit Input dialog opens.*


2. Make your edits. To view details for this input on the Input Details page, click the




(**View Details**) icon .

3. When finished, click **Save**.

## Delete an Input

1. In the applicable card, click the  (**Remove**) icon in the upper right corner of the applicable card.
2. In the Remove Input dialog, click **Remove**.

## Destinations

On the left edge of each card, the  (**Connected Inputs**) icon is displayed. This icon represents the number of inputs to which the destination is connected

## Add a Destination

To add or change a destination, complete the following steps:

1. Click **Add Destination** in the upper right corner of the Destinations list.

*The Add Destination panel opens.*

2. Choose the destination type from the drop-down list and click **Next**.

*The second Add Destination dialog opens.*

3. Complete the applicable fields and click **Add Destination**.

*The new destination card is now displayed in the Destination list on the Data Flow page.*

## Edit a Destination

1. In the applicable destination card, click the destination name.

*The Edit Destination panel opens.*

2. Make your edits. To view details for this destination on the Destination Details page,

click the  (**View Details**) icon .

3. Click **Save**.



## Delete a Destination

In the applicable destination card, click the  (**Remove**) icon.

## Connections




### Create a Connection

A connection always consists of just 1 input and 1 destination. However, note that an input can send data to more than one particular destination. You would simply create another connection to do that.

On the right edge of an Input card, either a  (**Plus**) icon or an  (**Connected Destinations**) icon is displayed.

- If a **Plus** icon is displayed, this indicates that the input has no connected destinations, and therefore no connections.
- The **Counter** icon displays the number of destinations to which the input is connected (which also indicates how many connections have been created for the input. When you hover over it, it changes to the **Plus** icon.

To create a connection, complete the following steps:

1. Click the  (**Plus**) icon or the  (**Connected Destinations**) icon located on the right side of the applicable Input card and drag to the  (**Connected Inputs**) icon on the applicable Destination card.


*The Connection panel opens. Use the **Track data received against these** field to add subnets over which you want this destination to received telemetry. Only traffic coming from exporter IPs within the specified subnet will be forwarded.*

2. Make your edits and click **Save**.

### Edit a Connection



You can edit only UDP inputs, and for these inputs you can edit only the entries in the **Track data received against these** field. Use this field to add subnets over which you want this destination to received telemetry. Only traffic coming from exporter IPs within the specified subnet will be forwarded.

1. Click the connection line between the applicable input and destination, then click the  (**Edit**) icon.

*The Connection panel opens.*

2. Make your edits and **click Save**.

## Delete a Connection

Click the connection line between the applicable input and destination, then click the  (**Remove**) icon.

*The input and destination are no longer connected, so telemetry will no longer be sent from this input to this destination.*

## Broker Nodes and Clusters

### Activate Broker Nodes and Clusters for an Input

1. Click **Assign to** on the card.

*The Assignments dialog opens.*



- For some inputs you can assign only one broker node. For NSG, VPC, and Flow Generator inputs, you cannot assign more than one broker node nor can you assign clusters.
- For a specific broker node, you can assign only one Flow Generator input, but you can assign multiple NSG and VPC inputs.
- You can assign multiple UDP inputs to a node or a cluster.

2. Make your assignments. To view details for this input on the Input Details page, click

the  (**View Details**) icon.

3. When finished, click **Assign Nodes**.

### Edit Assigned Broker nodes and Clusters

1. Click **Assigned to** on the card.

*The Assignment dialog opens.*

2. Make your edits and click **Save** when done.

---

# Destinations

Cisco Telemetry Broker supports sending telemetry to the following types of destinations:

- **UDP Destinations** A destination that receives UDP data at a specific IP address and port.
- **SCA Destination** A destination that points data to a customer-owned Secure Cloud Analytics account.

Configuring an SCA destination can limit system performance (in terms of uploaded FPS). Factors that can contribute to this are the size of flow records, the compression achievable for those flow records, and the bandwidth available for which to send telemetry from the broker nodes to Secure Cloud Analytics.


Under most circumstances, assuming less than 100 bytes per flow record, Cisco Telemetry Broker should be able to send:

- 40K FPS per broker node (assuming there exists 8 cores per broker node) for a virtual deployment.
- 300K FPS per broker node for a hardware deployment (M6).

Cisco Telemetry Broker sends telemetry to destinations. A connection describes the telemetry that a destination would like to receive from a particular telemetry stream.

From this page, you can add additional destinations as well as modify and update them. For each destination, you can add additional connections and receive telemetry from different telemetry inputs. You can configure multiple connections (1 telemetry input per connection) per destination.

You can see the following information on the Destinations page:

- Status.
- Destination name.
- Notifications.
- Destination type.
- Assigned inputs. (To see the list of inputs assigned to a destination, click the  **(Information)** icon.)
- The amount of telemetry sent to each destination for the last 24 hours.
- The combined rate of telemetry sent to each destination for the last 24 hours.

## How to Find This Page

From the Cisco Telemetry Broker main menu, choose **Destinations**.



## Import UDP Director Configuration

From either the UDP Director or the Manager that manages the UDP Director, you can export your current UDP Director destination and rule configuration as an XML file and import it into Cisco Telemetry Broker. For more details, see [Appendix C: Import UDP Director Configuration](#).




Once you have created your first destination, you no longer have the option to import a UDP Director configuration.




Importing a UDP Director configuration overwrites your current Cisco Telemetry Broker configuration, including all currently configured inputs, destinations, and rules.

## Filter Your Search

### Filter

Use the  (**Filter**) icon to filter your search for destinations.

1. Click the  (**Filter**) icon in the Destinations list.  
*The Filter Destinations dialog opens within which are filter options you can choose.*
2. Choose as many filters as necessary, and when you are finished, click **Apply**.
3. (Conditional) If you want to reset the settings to what they originally were before you began to make changes, click **Reset**.



When you use one or more filters, all filters are ANDed together; therefore, all returned results must match the search criteria for all of the filters.

### Clear Filters

- If you receive one or more results but do not see any for which you are searching, it could be that you have configured too many filters. In this instance, we recommend that you eliminate one filter at a time to see if any of your intended results show.
- If you want to clear all filters, click the **x** beside the Filter button.
- If you want to clear an individual filter field or apply additional filters, click the Filter button (which contains the number of filters applied). When the Filter Destinations panel opens, make your changes and click **Apply**. Click **Reset** to remove all filter criteria.

---

## Search

In the Search field, type the name of the destination for which you are searching. As you start to type your entry, the field dynamically filters to display a list of entries that contains any of the characters you have entered.

Keep in mind that you can create multiple destinations with the same name. Port numbers among broker nodes can also be duplicated. So if you search for a destination for which there are more than one with the same name, or search for a port number that has been duplicated on two or more broker nodes, all matching entries will be displayed after your search has finished processing.

## Sort Columns

Use the ▲ (**Move Up**) icon and the ▼ (**Move Down**) icon at the top of a column to reverse the sort order of the column.

## Add a Destination

### Add a UDP Destination

1. In the upper right corner of the page, click **Add Destination**.

*The Add Destination panel opens.*

2. Enter or select a destination type and click **Next**.
3. Configure all applicable fields and click **Add Destination**.
4. If you want to be alerted of destinations that are unreachable or unresponsive, enable the  (**Reachability Check**) icon (the bar is blue when enabled). For more information about the Reachability Check feature, see the next section, "Reachability Check."



- The Reachability Check feature is available only for non-Secure Cloud Analytics destinations.
- You can disable this feature on a per destination basis.
- Disable this feature if your destination or firewall rule configuration will result in false positive alerts.

## Reachability Check

The Reachability Check feature alerts users of destinations that are unreachable or unresponsive so they can mitigate any network damage caused by the forwarding of telemetry to a non-existent destination.

The feature crafts zero-length UDP packets and sends them to the configured UDP port of the destination. The broker node listens for ICMP Host Unreachable or Port Unreachable responses to determine if the destination is unreachable. The absence of any response indicates that the destination is most likely receiving telemetry.

For information about how to configure the amount of time before Cisco Telemetry Broker marks a telemetry input as inactive, see [General](#).

## Add a Secure Cloud Analytics (SCA) Destination



- In Cisco Telemetry Broker, you can add only 1 SCA Destination per system.
- Cisco Telemetry Broker extracts flow data from NetFlow V5, NetFlow V9, and IPFIX packets, and sends this data to Secure Cloud Analytics.
- If your Cisco Telemetry Broker deployment contains light telemetry, it may take up to 20 minutes for telemetry to appear on the Destinations page after you add an SCA destination.

Before you add an SCA destination, you need to obtain an SCA Service Key and the SCA Host URL. Secure Cloud Analytics uses this key to authenticate Cisco Telemetry Broker, and Cisco Telemetry Broker uses the URL to send telemetry to Secure Cloud Analytics.

### Locate the key and the URL

1. Log in to Secure Cloud Analytics.
2. From the main menu, click **Settings > Sensor**.
3. Locate and copy the Service key and the Service host at the bottom of the page. .



### Add the SCA destination

1. Log in to Cisco Telemetry Broker.
2. In the upper right corner of the page, click **Add Destination > SCA Destination**.
3. Enter a destination **Name**.
4. Enter the **SCA Service Key**. Ensure that you paste the entire key.
5. Enter the **SCA Host URL**. Ensure that you paste the entire URL.
6. Click **Save**.

Once you've configured Secure Cloud Analytics as a Cisco Telemetry Broker destination, you should be able to see telemetry from Cisco Telemetry Broker in the Secure Cloud Analytics Event Viewer within 30 minutes. If you do not, please contact [swatchc-support@cisco.com](mailto:swatchc-support@cisco.com) with your portal URL for assistance.

---


## Edit a Destination

1. In the row containing the applicable destination, click the  (**Edit**) icon.
2. Make your changes. To view details for this input on the Destination Details page, click the  (**View Details**) icon.
3. When finished, click **Save**.

## Remove a Destination

When you delete a destination, that destination is still available for selection in the metric graphs, but the name associated with it is the term "Destination" followed by the destination's ID and the phrase "deleted." For example, Destination (ID 10) deleted. The graphs still include data from the deleted destination as long as data exists for that destination. Once the data expires, the associated destination is no longer available for selection from any of the Per Destination drop-down lists (located on the Broker Nodes page).

To remove a destination, complete the following steps:

1. In the row containing the applicable destination, click the  (**Remove**) icon.  
*The Remove Destination dialog opens.*
2. Click **Remove**.

## View Details of a Destination

You can view more detailed information about a particular destination. To do this, in the row containing the applicable destination, click the destination name. For information about this page, see the next section, [Destination Details](#).

## Destination Details

On this page you can view more detailed information about a particular destination. To view the details of a destination, do the following:


- On the Destinations tab, click the desired destination name.

*The Destination Details page for that destination opens.*

On this page you can view the following information, depending on the destination type

### General Information

You can see the following information, depending on the destination type:

- Status.
- Destination type.
- Whether or not Reachability Check is enabled or disabled. If you want to be alerted of destinations that are unreachable or unresponsive, enable the  (**Reachability Check**) icon (the bar is blue when enabled). For more information about the Reachability Check feature, see the "Reachability Check" section in [Destinations](#).
- Destination IP address.
- Destination port number over which it receives telemetry.


## Notifications

All messages regarding this destination are displayed in this section. For example, if the destination has sent a "destination unreachable" ICMP message, you would see a notification about this here. The total number of notifications is in parentheses after the Notifications title.

## Sent Rate

- The amount of telemetry sent to this destination for the last 24 hours.
- The rate of telemetry sent to this destination for the last 24 hours.

## Edit a Destination

1. In the upper right corner of the page, click  **Edit Destination**.  
*The Edit Destination panel opens.*
2. Make your changes.
3. When finished, click **Save**.

## Remove a Destination

When you delete a destination, that destination is still available for selection in the metric graphs, but the name associated with it is the term "Destination" followed by the destination's ID and the phrase "deleted." For example, Destination (ID 10) deleted. The graphs still include data from the deleted destination as long as data exists for that destination. Once the data expires, the associated destination is no longer available for selection from any of the Per Destination drop-down lists (located on the Broker Nodes page).

To remove a destination, complete the following steps:

1. In the upper right corner of the page, click  **Remove Destination**.

*The Remove Destination Dialog opens.*

2. Click **Remove**.

## Connected Inputs/Exporters

The first number in the bubble following this title represents the total number of inputs assigned to this destination, and the second number represents the total number of exporters assigned to all inputs that are assigned to this destination.

Use the ▲ (**Move Up**) icon and the ▼ (**Move Down**) icon at the top of a column to reverse the sort order of the column.

Filter the table using the All option and the No Exporters option.

- Click **All** to see a list of all the inputs that are connected to this destination. The number in parentheses in the All button represents the total number of inputs assigned to this destination, and it should match the first number displayed in the bubble at the end of the "Connected Inputs/Exporters" title.
- Click **No Exporters** to see a list of only inputs that have no assigned exporters.

## Information Included in the Table


- Status, name, and type of input connected to this destination.
- Number of exporters sending data to a particular input, either on a single node or on multiple nodes.

Note that this number will not necessarily correspond to the second number displayed after the "Connected Inputs/Exporters" title. This, too, is the number of unique exporters sending data to a specific input. Refer to the following to determine whether or not these numbers will match:

- If a single exporter is sending data to a single node configured under the same input, then these numbers will match.
- If a single exporter is sending data to 2 nodes configured under the same input, then the number on the Destinations Details page will be double the number on the Input Details page.
- If a single exporter is sending data to 3 nodes configured under the same input, then the number on the Destinations Details page will be triple the number on the Input Details page, and so on.



The occurrence of these numbers not matching should rarely occur. To avoid this problem, we recommend that you configure inputs with only

 one broker node or one cluster. Conversely, you can create two separate UDP inputs that listen on the same UDP port but are assigned to different broker nodes or clusters.

- The amount of telemetry sent to this destination for the last 24 hours.
- The rate of telemetry sent to this destination for the last 24 hours.


## Metrics: Sent Rate

In the Metrics section you will see a Sent Rate table showing the rate at which inputs have sent telemetry to this destination over time.

You can view these metrics over different time frames (listed below) by clicking the buttons in the upper right corner (4 hours is the default):

- Last hour
- Last 4 hours
- Last day
- Last week
- Last month

You can filter the telemetry by the following entities (you can choose more than one option from each drop-down list):

 For SCA destinations, you can filter the telemetry in this table only per broker node or per the total amount received.

- Per Telemetry Type
- Per Input
- Per Exporter
- Per Broker Node
- Total

# Inputs

Cisco Telemetry Broker enables you to configure inputs to listen for different types of telemetry that you want processed. Refer to the following list for examples.

- If you want to collect UDP packets on port 2055 on all broker nodes, you should create a UDP Input configured to listen on port 2055.
- If you want to process VPC Flow Log telemetry, you should create a VPC Flow Log input and assign to it a broker node.
- If you want to process NSG Flow Log telemetry, you should create an NSG Flow Log input and assign to it a broker node.
- If you want to generate IPFIX records from raw network traffic, you should configure a monitor interface on a broker node to receive SPAN port traffic, create a Flow Generator input, and assign that input to the broker node.



To enable a virtual broker node to receive telemetry from a Flow Generator input, refer to the Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide for information about how to add more CPUs, memory, and a network interface to a broker node.



To begin collecting telemetry, you first need to create one or more Inputs within the Cisco Telemetry Broker and assign to it a minimum of one broker node.



You can forward telemetry from a Flow Generator input to SCA or UDP IPv4 destinations, but you should not configure a Flow Generator input to send telemetry to a UDP IPv6 destination, since this configuration combination is not currently supported.

You can see the following information on the Inputs page:

- Status.
- Input name.
- Notifications.
- Input type.
- Assigned broker nodes and destinations. (To see the list of the broker nodes and destinations assigned to an input, click the associated ⓘ (**Information**) icon.)
- The amount of telemetry received by each input for the last 24 hours.
- The combined rate of telemetry received by each input for the last 24 hours.




---

## How to Find This Page

From the Cisco Telemetry Broker main menu, choose **Inputs**.

## Filter Your Search

### Filter

Use the  (**Filter**) icon to filter your search for inputs.

1. Click the  (**Filter**) icon in the Inputs list.

*The Filter Inputs dialog opens within which are filter options you can choose.*

2. Choose as many filters as necessary, and when you are finished, click **Apply**. Note that in the Filter dialog for inputs, you also can filter by broker nodes and clusters.
3. (Conditional) If you want to reset the settings to what they originally were before you began to make changes, click **Reset**.



When you use one or more filters, all filters are ANDed together; therefore, all returned results must match the search criteria for all of the filters.

### Clear Filters

- If you receive one or more results but do not see any for which you are searching, it could be that you have configured too many filters. In this instance, we recommend that you eliminate one filter at a time to see if any of your intended results show.
- If you want to clear all filters, click the **x** beside the Filter button.
- If you want to clear an individual filter field or apply additional filters, click the Filter button (which contains the number of filters applied). When the Filter Inputs panel opens, make your changes and click **Apply**. Click **Reset** to remove all filter criteria.

### Search

In the Search field, type the name of the input for which you are searching. As you start to type your entry, the field dynamically filters to display a list of entries that contains any of the characters you have entered.

Keep in mind that you can create multiple inputs with the same name. Port numbers among broker nodes can also be duplicated. So if you search for an input for which there are more than one with the same name, or search for a port number that has been duplicated on two or more broker nodes, all matching entries will be displayed after your search has finished processing.

---

## Sort Columns

Use the ▲ (**Move Up**) icon and the ▼ (**Move Down**) icon at the top of a column to reverse the sort order of the column.

## Import UDP Director Configuration

From either the UDP Director or the Manager that manages the UDP Director, you can export your current UDP Director configuration as an XML file and import it into Cisco Telemetry Broker. For more details, see [Appendix C: Import UDP Director Configuration](#).



Once you have created your first destination, you no longer have the option to import a UDP Director configuration.



Importing a UDP Director configuration overwrites your current Cisco Telemetry Broker configuration, including all currently configured inputs, destinations, and rules.

## Add an Input

1. In the upper right corner of the page, click **Add Input**.

*The Add Input dialog opens.*

2. Select the input type and click **Next**.

*A second Add Input dialog opens.*

3. Configure all applicable fields and click **Add Input**. For information about the Disable Exporters Tracking toggle, see [Disable Exporters Tracking](#) (next section).

*The Assignments dialog opens.*

4. (Optional) Assign broker nodes or clusters to the input and click **Assign Nodes**. If a node is included in an HA Cluster, it will not be listed as a broker node.

*An input card for this input is now displayed in the Inputs list.*

If you don't assign broker nodes or clusters to the input at this step, you can do so

later on either this page by clicking the + (**Plus**) icon or the ⓘ (**Information**) icon in the Assigned Nodes column in the applicable input's row in the table, or by clicking the **Assign to** button in the applicable input card on the Data Flow page.

## Disable Exporters Tracking

If you are adding a UDP input type, you may want to turn on the Disable Exporters Tracking feature. To turn on Disable Exporters Tracking, click the **Disable Exporters Tracking** toggle (the toggle turns blue).



Exporters are tracked by default (Disable Exporters Tracking is turned off and toggle is gray).

Cisco Telemetry Broker tracks every exporter that sends telemetry to a UDP input. However, when you have many unique exporters sending telemetry to a single UDP input, you may need to turn on Disable Exporters Tracking to ensure the system does not suffer performance issues.

When you turn on Disable Exporters Tracking, metrics are no longer calculated for each exporter. However, you can still view the aggregate metrics that are being processed by the UDP input, though your system will have the following limitations:

- **Input Details page** The Exporters section no longer displays per-exporter metrics. (This page opens when you click a UDP input name on the Inputs page.) However, it will display the number of exporters seen by each broker node configured for the associated input.
- **Broker Nodes Details page** The Per Exporter drop-down list for the Received Rate graph no longer includes exporters from any UDP Inputs where exporter tracking has been disabled. (This page opens when you click a broker node name on the Broker Nodes tab.)

Although metrics are no longer calculated for each exporter, data for that exporter is still shown for as long as data exists (for the metrics database retention interval).



The data retention interval is a low-level database parameter and is not configurable from the interface.

*Example: The retention interval is 8 days. An exporter stopped sending data on August 10, so it will retain data from August 10-18. Today is August 20.*

- If you filter a chart for 7 days or 30 days, the chart continues to show data for that exporter, since August 10-18 falls within 7-30 days ago.
- If you filter a chart for 4 hours or 24 hours, the chart no longer shows data for that exporter, since August 10-18 falls outside those intervals.

---

## Edit an Input

1. In the row containing the applicable input, click the  (**Edit**) icon.

*The Edit Input dialog opens.*

2. Make your changes. To view details for this input on the Input Details page, click the



(**View Details**) icon.

3. When finished, click **Save**.

## Remove an Input

When you delete an input, Cisco Telemetry Broker stops receiving telemetry from that input and deletes any connections associated with this input.

That input is still available for selection in the metric graphs, but the name associated with it is the term "Input" followed by the Input's ID and the phrase "deleted." For example, Input (ID 10) deleted. The graphs still include data from the deleted input as long as data exists for that input. Once the data expires, the associated input is no longer available for selection from any of the Per Input drop-down lists (located on the Destinations and Broker Nodes pages).

To remove an input, complete the following steps:

1. In the row containing the applicable input, click the  (**Remove**) icon.

*The Remove Input dialog opens.*

2. Click **Remove**.

## View Details of an Input

You can view more detailed information about a particular input. To do this, in the row containing the applicable input, click the input name. For information about this page, see [Input Details](#).

## Broker Nodes and Clusters

### Activate Broker Nodes and Clusters

1. In the Assigned Nodes column for the applicable input, click the  (**Plus**) icon .

*The Assignments dialog opens.*



- For some inputs you can assign only one broker node. For NSG, VPC, and Flow Generator inputs, you cannot assign more than one broker node nor can you assign clusters.
- For a specific broker node, you can assign only one Flow Generator input, but you can assign multiple NSG and VPC inputs.
- You can assign multiple UDP inputs to a node or a cluster.

2. Make your assignments. To view details for this input on the Input Details page, click

the  (**View Details**) icon.

3. When finished, click **Assign Nodes**.

## Edit Assigned Broker Nodes and Clusters

1. In the Assignments column for the applicable input, click the  (**Information**) icon .

*The Assigned Broker Nodes/Clusters dialog opens, which lists the assigned broker nodes and clusters.*

2. Click **Edit**.

*The Assignments dialog opens.*

3. Make your edits and click **Save** when done.

## Input Details

On this page you can view the following detailed information about an input. To view the details of an input, do the following:

- On the Inputs page, in the row containing the applicable input, click the input name.

*The Input Details page for that input opens.*

On this page you can view the following information, depending on the input type:

### General Information

- Status.
- Input type.
- The number of assigned broker nodes and their names. To assign or edit broker nodes, click **Assign to** or **Assigned to** (whichever text is displayed). When the Assignments panel opens, make your changes, and when you are finished, click **Save**.

---

## Notifications

All messages regarding this input are displayed in this section. For example, when an input doesn't have a broker node assigned to it, or an input isn't connected to a destination, you would see a notification about this here. The total number of notifications is in parentheses after the Notifications title.


## Received Rate

- The amount of telemetry received by this input for the last 24 hours.
- The rate of telemetry received by this input for the last 24 hours.

## More Details

Click the drop-down arrow to view additional information about the input. This information varies depending on the input type. Examples of details are input name, blob service SAL URL, and IP address.

## Edit an Input

1. In the upper right corner of the page, click  **Edit Input**.

*The Edit Input panel opens.*

2. Make your changes.
3. When finished, click **Save**.

## Remove an Input

When you delete an input, Cisco Telemetry Broker stops receiving telemetry on the specified port and deletes any connections associated with this input.

That input is still available for selection in the metric graphs, but the name associated with it is the term "Input" followed by the Input's ID and the phrase "deleted." For example, Input (ID 10) deleted. The graphs still include data from the deleted input as long as data exists for that input. Once the data expires, the associated input is no longer available for selection from any of the Per Input drop-down lists (located on the Destinations and Broker Nodes pages).

To remove a UDP input, complete the following steps:

1. In the upper right corner of the page, click  **Remove Input**.

*The Remove Input Dialog opens.*

2. Click **Remove**.

## Connected Destinations

Use the ▲ (**Move Up**) icon and the ▼ (**Move Down**) icon at the top of a column to reverse the sort order of the column.

This section includes the following information, depending on the destination type:

- Total number of destinations connected to this input. (This number is displayed after the "Connected Destinations" title.)
- Status
- List of destinations connected to this input and their details.
- Input type.
- The amount of telemetry sent to this destination for the last 24 hours.
- The rate of telemetry sent to this destination for the last 24 hours.

## Create a Connection



A connection always consists of just 1 input and 1 destination. However, note that an input can send data to more than one particular destination. You would simply create another connection to do that.

1. In the upper right corner of the table, click + **Connect to**.  
*The Connect to a Destination panel opens.*
2. Choose the destination.
3. (Conditional) If you choose a UDP input, the **Track data received against these subnets** field opens. This field serves as a filter mechanism to determine which traffic is sent to the destination. Only traffic coming from exporter IPs within the specified subnet will be forwarded. Enter the subnets over which this destination will receive the applicable telemetry. Separate entries with a comma.

If you leave the **Track data received against these subnets** field empty, it will default to a single subnet that includes all traffic.

- For IPv4 IP subnets, the CIDR IP address range will be 0.0.0.0/0.
- For IPv6 IP subnets, the CIDR IP address range will be ::/0.

4. Click **Save**.

## Edit a Connection



You can only edit connections to a destination if the input is UDP, and for these inputs you can edit only the entries in the **Track data received against these**




**subnets** field. Use this field to add subnets over which you want this destination to received telemetry. Only traffic coming from exporter IPs within the specified subnet will be forwarded.

1. To edit a connection, click the  (**Edit**) icon at the end of the applicable row.

*The Connect to Destination panel opens.*

2. Make your edits and click **Save**.

## Remove a Connection

1. To remove a connection, click the  icon at the end of the applicable row.
2. Click **Remove**.

## Metrics

In the Metrics section you will see a Received Rate table showing the rate at which this input has received telemetry over time.

You can view these metrics over different time frames (listed below) by clicking the buttons in the upper right corner (4 hours is the default):

- Last hour
- Last 4 hours
- Last 24 hours
- Last week
- Last month

You can filter the telemetry by the following entities (you can choose more than one option from each drop-down list):

- Per Exporter
- Per Broker Node

## Exporters

In this section you can see the following information:

- The number of unique exporters (represented by the number in the bubble at the end of the Exporters title).
- Status




- Exporter IP address.
- Telemetry type.
- Number of destinations.
- The amount of telemetry received from each exporter for the last 24 hours.
- The rate of telemetry received from each exporter for the last 24 hours.

## Search

In the Search field, type the name of the exporter for which you are searching. As you start to type your entry, the field dynamically filters to display a list of entries that contains any of the characters you have entered.

## Filter

Use the  (**Filter**) icon to filter your search by status and telemetry type.

- If you want to clear all filters, click the **x** beside the Filter button.
- If you want to clear an individual filter field or apply additional filters, click the Filter button (which contains the number of filters applied). When the Filter Exporters panel opens, make your changes and click **Apply**. Click **Reset** to remove all filter criteria.



When you use one or more filters, all filters are ANDed together; therefore, all returned results must match the search criteria for all of the filters.

## Disable Exporters Tracking

If you are adding a UDP input type, you may want to turn on the Disable Exporters Tracking feature. To turn on Disable Exporters Tracking, click the **Disable Exporters Tracking** toggle (the toggle turns blue).



Exporters are tracked by default (Disable Exporters Tracking is turned off and toggle is gray).

Cisco Telemetry Broker tracks every exporter that sends telemetry to a UDP input. However, when you have many unique exporters sending telemetry to a single UDP input, you may need to turn on Disable Exporters Tracking to ensure the system does not suffer performance issues.

When you turn on Disable Exporters Tracking, metrics are no longer calculated for each exporter. However, you can still view the aggregate metrics that are being processed by the UDP input, though your system will have the following limitations:

- **Input Details page** The Exporters section no longer displays per-exporter metrics. (This page opens when you click a UDP input name on the Inputs page.) However, it will display the number of exporters seen by each broker node configured for the associated input.
- **Broker Nodes Details page** The Per Exporter drop-down list for the Received Rate graph no longer includes exporters from any UDP Inputs where exporter tracking has been disabled. (This page opens when you click a broker node name on the Broker Nodes tab.)

Although metrics are no longer calculated for each exporter, data for that exporter is still shown for as long as data exists (for the metrics database retention interval).



The data retention interval is a low-level database parameter and is not configurable from the interface.

*Example: The retention interval is 8 days. An exporter stopped sending data on August 10, so it will retain data from August 10-18. Today is August 20.*

- If you filter a chart for 7 days or 30 days, the chart continues to show data for that exporter, since August 10-18 falls within 7-30 days ago.
- If you filter a chart for 4 hours or 24 hours, the chart no longer shows data for that exporter, since August 10-18 falls outside those intervals.

## Add a Flow Generator Input



You need to specify the telemetry interface IP before you add a Flow Generator input.

For information about this, see the "Enable a Flow Generator Input on a Broker Node (Optional)" section in the Virtual Appliance Deployment and Configuration Guide.

---

# Broker Nodes

The Cisco Telemetry Broker Nodes Overview shows details about all of your broker nodes, including the following:

- Broker node name
- Admin interface (Management Network) IPv4/IPv6 addresses
- Telemetry interface IPv4/IPv6 addresses
- Capacity of the broker node
- The high availability cluster to which the broker node belongs (if any)
- Received and Sent rate in bps
- Status of the broker node and the last time the Manager node communicated with it

You can filter this telemetry by the following criteria. Simply choose one of the following criteria types from the drop-down menu at the top of the page:

- Highest Received Rate
- Most Recently Seen

In the Search field, the placeholder text informs you for which columns you can perform a search. As you start to type your entry, the table dynamically filters to display a list of entries that contain the characters you have entered.

## Add a Cluster

For cluster-related information and tasks, see [High Availability Clusters](#) and [Cluster Tasks](#).

## View Details of a Broker Node

You can view more detailed information about a particular broker node. To do this, in the applicable row, click the desired broker node name in the Broker Node Name column. For information about this page, see the next section, [Broker Node Details](#).

## Broker Node Details

To view the details of a broker node, do the following:

- On the Broker Nodes page, in the Broker Nodes table, click the applicable broker node name in the Broker Node Name column.

## General Section

This section contains the following information:

- 
- Host name and management network IP address
  - Status of the input and the last time it received telemetry
  - Received rate (in bytes per second) for the last 24 hours
  - Sent rate (in bytes per second) for the last 24 hours

## Telemetry Interface

This section contains the following information:

- Interface index
- Interface name
- MAC address
- PCI address
- Capacity (bps)
- IPv4 address/subnet prefix length
- IPv4 gateway address
- IPv6 address/subnet prefix length
- IPv6 gateway/address
- Interface MTU (bytes)

## Monitor Interface

By default, the monitor interface is not selected. If you will be assigning a flow generator input to a particular broker node, then you need to select the monitor interface and configure its mtu. To do this, run `ctb-install --config` on the broker node.


 A broker node supports only one monitor interface.

This section contains the following information:

- Interface index
- Interface name
- MAC address
- PCI address
- Capacity (bps)
- Interface MTU (bytes)

## Edit a Broker Node

To edit a broker node, complete these steps:

1. In the Telemetry Interface section, click the  (**Edit**) icon and make your desired changes.
2. Click **Save**.

## Remove a Broker Node


When you remove a broker node from the Manager node, that broker node is deleted from the database, and it is no longer assigned to any of the inputs and destinations to which it was previously assigned. Though the broker node is still available for selection in the metric graphs, the name associated with it changes to the term "Broker Node" followed by the Broker Node's ID and the phrase "deleted." For example, Broker Node (ID 10) deleted.

The graphs still include data from the deleted broker node as long as data exists for that broker node. Once the data expires, the associated broker node is no longer available for selection from any of the Per Broker Node drop-down lists (located on the Destinations and Inputs pages).

Note the following connections regarding the removal of a broker node:

- To ensure that the configuration information is deleted, you must run `ctb-manage` and select **deactivate**.
- If you do not complete the actions described in the previous bullet, the broker node continues to run with the previously saved configuration, and it does so without sending statistics to the Manager node.
- If you add back a previously deleted broker node to the same Manager node, you still need to configure it as a new appliance (assign a telemetry IP address, assign inputs, etc.)

To remove a broker node, complete these steps:

1. In the upper right corner, click the  (**Remove Broker Node**) icon.
2. In the Remove dialog, click **Remove**.



## Metrics

Details of the Metrics information are described below. The Metrics section shows telemetry this broker node receives over time, both by input and by destination.

### Received Rate table

This table shows telemetry that this broker node has received over time, per the following filters you can use to filter the telemetry. You can choose more than one option from each

drop-down list.



- Per Input
- Per Exporter
- When the **Compare to Capacity Toggle** icon is disabled () , you can view the current Received Rate values (in 1-minute intervals) for telemetry received from the applicable input(s) . (You must first click **Last 1h** from the time frame options bar in the upper right corner of the table.) Move your cursor over the x\_axis (the horizontal line that reflects the time) to find a specific minute in time.
- When the **Compare to Capacity Toggle** icon is enabled () , you can view the Received Rate values as they compare to the threshold. Rates that exceed the 90 percent threshold need to be investigated, as these are cause for concern.

You can view these metrics over several time frames by clicking any of the following desired time frames in the upper right corner of the table:

- Last hour
- Last 4 hours
- Last day
- Last week
- Last month

### Sent Rate table

This table shows telemetry that this broker node has sent over time to the destination(s) you select from the **Per Destination** drop-down list.

- When the **Compare to Capacity Toggle** icon is disabled () , you can view the current Sent Rate values (in 1-minute intervals) for telemetry sent to the applicable destination(s) . (You must first click **Last 1h** from the time frame options bar in the upper right corner of the table.) Move your cursor over the x\_axis (the horizontal line that reflects the time) to find a specific minute in time.
- When the **Compare to Capacity Toggle** icon is enabled () , you can view the Sent Rate values as they compare to the threshold. Rates that exceed the 90 percent threshold need to be investigated, as these are cause for concern.



If the received rate or sent rate are exceeding the threshold, add an additional broker node to increase capacity.

You can view these metrics over several time frames by clicking any of the following desired time frames in the upper right corner of the table:

- Last hour
- Last 4 hours
- Last day
- Last week
- Last month

### 1-Minute Load Average table

CPU load average of the chosen broker node over 1-minute intervals of time. (You must first click **Last 1h** from the time frame options bar in the upper right corner of the table.) Move your cursor over the x\_axis (the horizontal line that reflects the time) to find a specific minute in time. When the load average exceeds the threshold, which is set to the number of CPUs (the value represented by the y\_axis), your network telemetry flow rate slows down.

### Memory Usage table

Memory consumption and total available memory over 3-minute intervals of time. (You must first click **Last 1h** from the time frame options bar in the upper right corner of the table.) Move your cursor over the x\_axis (the horizontal line that reflects the time) to find a specific 3-minute interval in time. Rates that exceed the 80 percent threshold need to be investigated, as these are cause for concern.

### Disk Storage table

Disk storage used and total available storage over 3-minute intervals of time. (You must first click **Last 1h** from the time frame options bar in the upper right corner of the table.) Move your cursor over the x\_axis (the horizontal line that reflects the time) to find a specific 3-minute interval in time. Rates that exceed the 80 percent threshold need to be investigated, as these are cause for concern.



If you find that the load average, memory usage, or disk storage are exceeding the associated threshold, expand the resource allocation for your VM.

---

# High Availability Clusters

Cisco Telemetry Broker high availability provides highly available IPv4 and IPv6 virtual IP addresses to be targets for your inputs, ensuring reliable delivery of telemetry from inputs to destinations.

To establish Broker Node high availability, you can create high availability clusters and assign multiple broker nodes to each. In each cluster, one broker node is designated *Active*, meaning it passes telemetry and serves metrics to Cisco Telemetry Broker, and the rest are designated *Passive*, meaning they are not passing telemetry or serving metrics currently. If an Active broker node stops passing telemetry or otherwise loses connectivity with Cisco Telemetry Broker, one of the Passive broker nodes is promoted to Active broker node and starts passing telemetry.

Note the following about clusters:

- Each broker node can only belong to one cluster at a time.
- You can create a cluster without assigning a broker node, but note that the cluster will not receive telemetry until you add a node.
- You can assign an input to an empty cluster, but note that the cluster will not receive telemetry until you add a node.
- When you remove a broker node from a cluster, that node no longer has any inputs assigned to that cluster.
- Keep in mind that if you create a cluster with only one broker node and this broker node fails, no other broker node is available to be promoted to Active broker node. Similarly, if all broker nodes within a cluster fail, no broker node can be promoted to Active broker node. If a broker node fails, bring it back online as soon as possible.
- You cannot choose which broker node is active in a given cluster.
- If an Active broker node for a virtual IP address fails, one of the Passive broker nodes in the same cluster becomes the Active broker node for the virtual IP address. When the failed broker node comes back up again, it remains a Passive broker node. If you want to make that node active again, you will need to do so manually using the provided commands. (To view these commands, see the "Move a VIP to a Specific Node" section in the Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide.)
- You can assign either a virtual IPv4 or virtual IPv6 address, or both, to a cluster. Cisco Telemetry Broker uses this virtual IP address to communicate with the cluster and promote Passive broker nodes to Active broker nodes when an Active broker node loses connectivity with Cisco Telemetry Broker.



---

For information about how HA clusters are updated during the Cisco Telemetry Broker software update process, see [Software Update](#).

## Cluster Tasks

### View Cluster Details

In the High Availability Clusters section on the Broker Nodes page, you can view the following data:

- All configured clusters
- IPv4 address and IPv6 address for each cluster
- Broker nodes that belong to each cluster


### Add a Cluster

1. From the Cisco Telemetry Broker main menu, choose **Broker Nodes**.
2. On the right side of the page, click **+ Add Cluster**.
3. Enter a descriptive cluster name.
4. Choose one or more broker nodes to include in the cluster.
5. Enter a cluster virtual IPv4 Address, IPv6 Address, or both.
6. Click **Add Cluster**.




- It can take up to 3 minutes for the configuration to propagate and for the VIP addresses to become available on your network.
- The **+Add Cluster** button is disabled when no broker nodes are available to be assigned to a cluster.

### Modify a Cluster's Configuration

1. From the Cisco Telemetry Broker main menu, choose **Broker Nodes**.
2. In the High Availability Clusters section, click the  **(Edit)** icon for the cluster you want to edit.
3. In the Edit dialog that opens, make your edits and click **Save**.

## Remove a Cluster

1. From the Cisco Telemetry Broker main menu, choose **Broker Nodes**.
2. In the High Availability Clusters section, click the  **(Remove)** icon for the cluster you want to delete.
3. In the Remove dialog that opens, click **Remove**.

For information about managing clusters, refer to the "Manage High Availability Clusters" section in the Cisco Telemetry Broker Virtual Deployment Guide.

---

# Manager Node

The Cisco Telemetry Broker Manager view shows metrics for your Cisco Telemetry Broker Manager. You can view the following information:

- Hostname and Admin interface (Management Network) IPv4/IPv6 addresses
- Current memory use and total memory available
- Current disk storage use and total disk storage space available

## How to Find This Page

From the Cisco Telemetry Broker main menu, choose **Manager Node**.

### 1-Minute Load Average table

CPU load average of the chosen broker node over 1-minute intervals of time. (You must first click **Last 1h** from the time frame options bar in the upper right corner of the table.) Move your cursor over the x\_axis (the horizontal line that reflects the time) to find a specific minute in time. When the load average exceeds the threshold, which is set to the number of CPUs (the value represented by the y\_axis), your network telemetry flow rate slows down.

### Memory Usage table

Memory consumption and total available memory over 1-minute intervals of time. (You must first click **Last 1h** from the time frame options bar in the upper right corner of the table.) Move your cursor over the x\_axis (the horizontal line that reflects the time) to find a specific 3-minute interval in time. Any rate that exceeds the 80 percent threshold need to be investigated, as these are cause for concern.

### Disk Storage table

Disk storage used and total available storage over 3-minutes intervals of time. (You must first click **Last 1h** from the time frame options bar in the upper right corner of the table.) Move your cursor over the x\_axis (the horizontal line that reflects the time) to find a specific 3-minute interval in time. Any rate that exceeds the 80 percent threshold need to be investigated, as these are cause for concern.



If you find that the load average, memory usage, or disk storage are exceeding the associated threshold, expand the resource allocation for your VM.

You can view these metrics over several time frames by clicking any of the following desired time frames in the upper right corner of the Metrics table:

- Last hour
- Last 4 hours
- Last day
- Last week
- Last month

---

# Application Settings

The Application Settings control your Cisco Telemetry Broker deployment. The following settings are available:

## General


## Software Update

## Smart Licensing

## TLS Certificate

## User Management

## General

1. Click the  (**Settings**) icon.  
*The Application Settings page opens.*
2. Click the **General** tab.

## Configure Inactivity Interval

The telemetry inputs configuration allows you to configure the amount of time before Cisco Telemetry Broker marks a telemetry input as inactive.

1. In the Inputs section, choose an **Inactivity Interval** in minutes from the Inactivity interval drop-down list.
2. Click **Save**.

## Configure HTTPS Proxy

The HTTPS Proxy configuration allows you to configure HTTPS proxy server settings if Cisco Telemetry Broker connects to the internet using an HTTPS proxy.

 Cisco Telemetry Broker does not support using HTTP proxy servers.

1. In the HTTPS Proxy section, enable **Use HTTPS proxy**.
2. Enter an **IP Address** and **Port**.
3. Click **Save**.

## Software Update

The Software Update page shows the current Cisco Telemetry Broker version of your Manager node and broker nodes, and it allows you to upgrade to the current released

version.

The update upgrades your Manager and all of your managed broker nodes to the newest version. Before performing the update, we recommend that you take a VM snapshot of your Cisco Telemetry Broker VMs. You can use this snapshot to revert to the current state in case you receive an unexpected error.

The system is unresponsive during the update process. First it updates your Manager, and then it updates the broker nodes. While your Manager updates, you may not see the proper state of your Cisco Telemetry Broker deployment. While your broker nodes update, they may not properly pass sent telemetry to destinations.

The Cisco Telemetry Broker HA cluster is designed to ensure there is no down time during an upgrade; therefore, in an HA cluster, the Manager always updates only one node at a time. When updating an HA cluster, the Manager node updates nodes in that cluster by order of creation. When a node starts to update, it first puts itself into standby mode. If this is the active node, the Cisco Telemetry Broker functionality is transferred to the alternate node. This occurs before the previously active node stops processing telemetry. This ensures that there is minimal to no telemetry loss during an upgrade.



There are several issues that you need to be aware of when upgrading to v2.1.3 to ensure a successful upgrade. For more information, refer to the v2.1.3 Release Notes.

## Upgrade Your Cisco Telemetry Broker Deployment

### Download the Update File

1. Go to [Cisco Software Central](#).
2. In the Download and Upgrade section, choose **Access Download**.
3. Type **Cisco Telemetry Broker** in the search field.
4. Choose the **Manager Node Software**.
5. Download the CTB Update Bundle file.

### Upload the Update File

1. In the Cisco Telemetry Broker Manager, click the ⚙️ **(Settings)** icon.  
*The Application Settings page opens.*
2. Click the **Software Update** tab.
3. In the upper right corner of the page, click **Upload an Update File**.
4. Choose the file you downloaded.

---

*You may need to wait several minutes for the upload to finish, based on the time estimates displayed. After the file is uploaded, you will receive a message informing you that a software update is now available.*

5. Click **Update Cisco Telemetry Broker**.

*You will not be able to navigate within Cisco Telemetry Broker while the Manager node is updated to the latest version. The update process takes about 10 minutes.*

6. When the update has completed, you will be prompted to log back in to Cisco Telemetry Broker.

*A loading indicator will appear next to each broker node that is being updated.*

## Smart Licensing

The Smart Software Licensing page shows the state of your Cisco Telemetry Broker Smart Licensing.

Cisco Telemetry Broker licensing is based on GB ingested by your broker nodes per day.

1. Click the  **(Settings)** icon.

*The Application Settings page opens.*

2. Click the **Smart Licensing** tab.

## User Management

1. Click the **Settings** icon.

*The Application Settings page opens.*

2. Click the **User Management** tab.

## Add a User

1. Click **Add User**.

2. Enter the user's **First Name** and **Last Name**.

3. Enter the **Username**. Neither you or the user can change this username once it is created.

4. Enter a password in the **New Password** field and enter it again in the **Confirm Password** field. Make sure to adhere to the password guidelines.

5. Click **+ Add User**.

---

## Edit a User

1. In the row that contains the user you want to edit, click the **⋮ (Actions)** icon > **Edit Profile**.
2. Complete your edits.
3. Click **Save**.

## Remove a User

1. In the row that contains the user you want to remove, click the **Actions** icon > **Remove User**.
2. Click **Remove**.

## Change a User's Password

1. In the row that contains the user whose password you want to change, click the **Actions** icon > **Change Password**.
2. Enter a new password in the **Password** field, and enter it again in the **Confirm Password** field.
3. Click **Change Password**.

## TLS Certificate


On this page you can view the following information:

- Hostname
- Certificate expiration date and time
- Subject name and issuer name (under Certificate details)

 The certificate and the private key must be PEM-encoded.

 The private key file cannot be password-protected.

## Upload TLS Certificate

1. Click the  **(Settings)** icon.  
*The Application Settings page opens.*
2. Click the **TLS Certificate** tab.
3. To view certificate details, click the **Certificate details drop-down arrow**. In this section you can view the Subject Name, Issuer Name, and Subject Alternate Name.



4. In the upper right corner of the page, click **Upload TLS Certificate**.
5. In the Upload TLS certificate dialog that opens, click **Choose File** for each certificate and each private key you want to upload.

*Certificate details are displayed beneath the associated files so you can verify that all related information is correct.*

6. Click **Upload**.

## Re-register Broker Nodes

After you upload the appropriate TLS certificates, you need to enable the connection between the Manager node and the broker nodes by re-registering each broker node.

1. Use SSH or the VM server console to log in to the appliance as **admin**.
2. Enter this command:

```
sudo ctb-manage
```

You are informed that a Manager configuration already exists.

3. Choose **Option C "Re-fetch the manager's certificate but keep everything else"**.

## Syslog Notifications

1. Click the  **(Settings)** icon.

*The Application Settings page opens.*

2. Click the **Notifications** tab.

To see a list of supported alerts, click the **Supported Alerts drop-down arrow** at the top of the page. You can direct Cisco Telemetry Broker to send a syslog notification when any alert is generated. For a list of these alerts, refer to [Appendix B: Supported Alerts](#).

 Currently you cannot configure custom alert types.

## Configure the Syslog Server

First, you need to configure the Syslog server settings.

1. In the Syslog Server Address field, click **Configure**.
2. Enter the applicable Syslog server address (this can be an IPv4 address, IPv6 address, or a DNS name) and port number.
3. Click **Save**.

## Enable the Syslog Server to Receive Notifications

Next, do the following:

- Enable the **Send Syslog Notifications** toggle ()

After you configure the Syslog server, you must enable this toggle, or the Syslog server will not receive notifications. Once you have enabled this toggle, then when your Cisco Telemetry Broker triggers an alert, it immediately sends a syslog notification to the Syslog server.

## Send a Test Syslog Notification

Whenever you choose to do so, you can manually send a test syslog notification to the syslog server. This test notification checks that the Syslog server is successfully receiving syslog messages.


Every time you send a test syslog notification, a copy of the message appears under the **Sent Test** button. This enables you to compare the sent message with the message that the Syslog server receives.

If you log out of Cisco Telemetry Broker, when you log in again the messages will no longer be displayed.



You must manually check the syslog server to verify that a test notification was received.


To send a test syslog notification, complete the following steps:

1. Enable the **Send Syslog Notifications** toggle ()
2. Click **Send Test**.
3. In the confirmation dialog, click **Send**.

## Severity and Facility Values

Telemetry Broker hardcodes the severity value to *warning* and the facility value to *local0*.

## Email Notifications

1. Click the  (**Settings**) icon.  
*The Application Settings page opens.*
2. Click the **Notifications** tab.

You can direct Cisco Telemetry Broker to send an email notification when any alert is generated. For a list of these alerts, refer to [Appendix B: Supported Alerts](#).

 Currently you cannot configure custom alert types.


## Configure the SMTP Server

First, you need to configure the SMTP server settings.

1. In the SMTP Server field, click **Configure**.
2. Enter the applicable SMTP server address (this can be an IPv4 address, IPv6 address, or a DNS name), port number, and the email address from which the alerts will be sent.
3. Designate whether or not you want to require authentication. If you do, enter the SMTP server's username and password into the associated fields.
4. Choose the encryption type.
5. Click **Save**.


## Enable a User to Receive Email Notifications

After you configure the SMTP server, you must enable Cisco Telemetry Broker to send email notifications, or the designated users will not receive notifications.

1. Enable the **Send Email Notifications** toggle ()
2. In the Recipients field, click **Edit**.
3. In the Edit Recipients dialog that opens, choose every user whom you want to have the ability to receive email notifications.
4. Click **Save**.

## Send a Test Email Notification

Whenever you choose to do so, you can manually send a test email notification for all alerts. This test email notification checks that the SMTP server has been correctly configured and that all appropriate users will successfully receive email notifications for any alerts (to which they are assigned) that occur.

1. Enable the **Send Email Notifications** toggle ()
2. Click **Send Test**.
3. If you need to edit the list of users who will receive this test email notification, then in the Send Test dialog that opens, click **Choose** and make your edits.
4. Click **Send**.


---

# Profile Settings

## Edit Your Personal Information

1. Click the  (**User**) icon.

*The Profile Settings page opens.*

2. In the Personal Information section, click the  (**Edit**) icon.
3. Complete your edits.
4. Click **Save**.

## Change Your Password

1. Click the **User** icon.

*The Profile Settings page opens.*

2. In the Password section, click **Change Password**.
3. Enter a new password in the **Password** field, and enter it again in the **Confirm Password** field.
4. Click **Change Password**.

# Expand Cisco Telemetry Broker Manager and Broker Node Disk Size

With Cisco Telemetry Broker, you can expand the disk size of both the Manager and any broker node.

## 1. Back Up the Partition Table Information

Log in to the appliance and run the following command.

```
admin@ctb-nfik72TO:~$ sudo sgdisk -p /dev/sda > partition_table_$(date +%Y_%m_%d_%H_%M_%S').txt
```

This creates a file similar to the `partition_table_2021_07_09_15_51_04.txt` file, with contents similar to the following:

```
Disk /dev/sda: 81920000 sectors, 39.1 GiB
Model: Virtual disk
Sector size (logical/physical): 512/512 bytes
Disk identifier (GUID): B078BED8-2BD0-4EEA-9149-BA93FC8A299D
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 81919966
Partitions will be aligned on 2048-sector boundaries
Total free space is 4029 sectors (2.0 MiB)
```

Number	Start (sector)	End (sector)	Size	Code	Name
1	2048	4095	1024.0 KiB	EF02	
2	4096	491519	238.0 MiB	8300	
3	491520	3844095	1.6 GiB	8200	
4	3844096	33767423	14.3 GiB	8300	
5	33767424	63690751	14.3 GiB	8300	
6	63690752	81917951	8.7 GiB	8300	




The total size of the disk (`/dev/ada`) is 39.1 GB and the size of the Cisco Telemetry Broker application partition (`/dev/sda6`) is 8.7 GB.

## 2. Delete All Existing VM Snapshots for the Appliance

You cannot resize the ESXi VM disk when snapshots exist. In order to increase the disk size we need to delete all existing snapshots.

1. Log in to the ESXi console (vSphere or Web Client).
2. Right-click the VM and choose **Snapshots > Manage Snapshots > Delete All**.

### 3. Increase the Disk Size of the Appliance

1. Log in to the ESXi console (vSphere or Web Client).
2. From the list of VMs in the left panel, select the appliance.
3. From the toolbar at the top of the page, click the  (Edit) icon.
4. In the Hard Disk 1 row, increase to the desired size.
5. Reboot the VM.
6. Log in and verify that the new size has been applied by running this command:

```
$ sudo sgdisk -p /dev/sda
Disk /dev/sda: 125829120 sectors, 60.0 GiB
Model: Virtual disk
Sector size (logical/physical): 512/512 bytes
Disk identifier (GUID): B078BED8-2BD0-4EEA-9149-BA93FC8A299D
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 81919966
Partitions will be aligned on 2048-sector boundaries
Total free space is 4029 sectors (2.0 MiB)
```

Number	Start (sector)	End (sector)	Size	Code	Name
1	2048	4095	1024.0 KiB	EF02	
2	4096	491519	238.0 MiB	8300	
3	491520	3844095	1.6 GiB	8200	
4	3844096	33767423	14.3 GiB	8300	
5	33767424	63690751	14.3 GiB	8300	
6	63690752	81917951	8.7 GiB	8300	

### 4. Run ctb-part-resize.sh Script

1. Take a snapshot of the VM.
2. Run the following command:

```
$ sudo /opt/titan/bin/ctb-part-resize.sh

WARNING

This program will update /dev/sda6 to use the full remaining free space
available on /dev/sda.

It is HIGHLY RECOMMENDED that you take a backup of any important data/configuration
before proceeding.

Do you wish to proceed?y
<134>Mar  8 15:35:30 ctb-disk-resize: Moving the partition table header to the end of the
disk(/dev/sda)
```

```
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot or after you
run partprobe(8) or kpartx(8)
The operation has completed successfully.
<134>Mar  8 15:35:31 ctb-disk-resize: Deleting CTB application partition (/dev/sda6)
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot or after you
run partprobe(8) or kpartx(8)
The operation has completed successfully.
<134>Mar  8 15:35:32 ctb-disk-resize: Creating the CTB application partition (/dev/sda6)
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot or after you
run partprobe(8) or kpartx(8)
The operation has completed successfully.
<134>Mar  8 15:35:33 ctb-disk-resize: Updating kernel partition tables
<134>Mar  8 15:35:34 ctb-disk-resize: Resizing /dev/sda6
resize2fs 1.44.5 (15-Dec-2018)
Filesystem at /dev/sda6 is mounted on /var/lib/titan; on-line resizing required
old_desc_blocks = 2, new_desc_blocks = 2
The filesystem on /dev/sda6 is now 2412283 (4k) blocks long.
```

## 5. Verify that Space has been Allocated

Run the following command:

```
$ df -h /dev/sda
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda4       14G   5.6G  7.7G  42% /
/dev/sda2       227M   80M  132M  38% /boot
/dev/sda5       14G   41M   14G   1% /mnt/alt_root
/dev/sda6       8.5G  172M   7.9G   3% /var/lib/titan
```

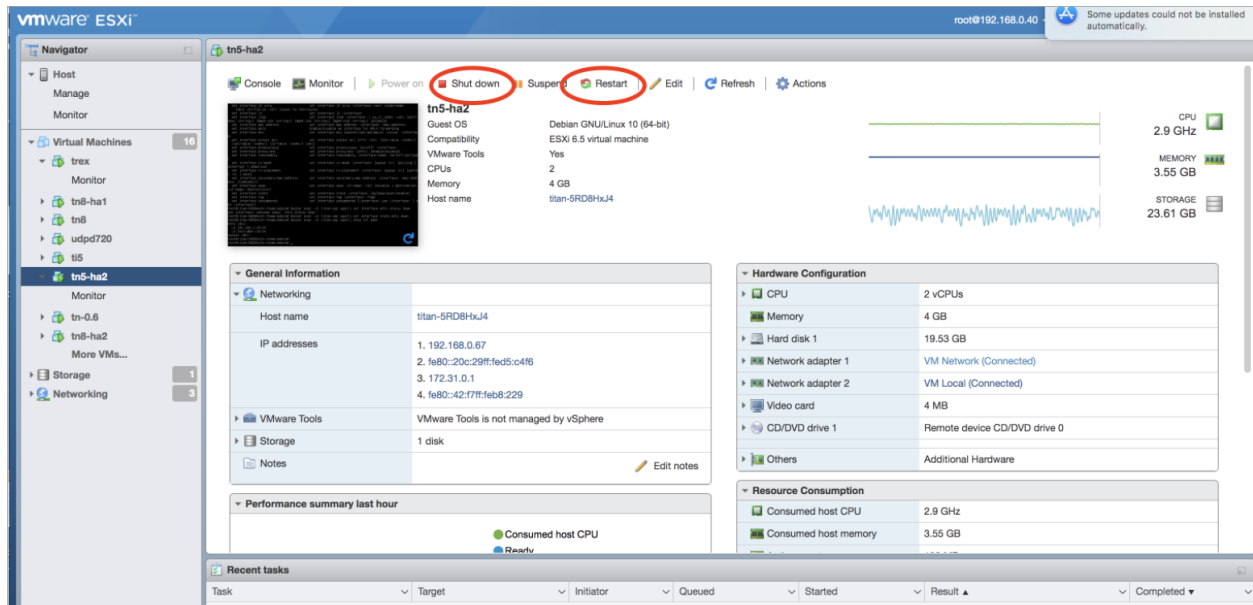
# Shut Down or Reboot Cisco Telemetry Broker

If at some point you need to shut down or reboot Cisco Telemetry Broker, complete the following steps:

1. Log in to the CTB Manager or CTB Broker Node via ssh or the console with the user name **admin**.
  - To shut down, enter `sudo shutdown now`
  - To reboot, enter `sudo shutdown -r now`
2. Log in to the VMWare console and verify that the VM has completed the shutdown or has rebooted properly.

Optionally, you can also shut down or reboot using VMWare. To do this, complete the following steps:

1. Log in to the VMWare console and select the applicable VM.
2. Depending on if you want to shut down or reboot, click one of the following options displayed at the top of the page:





# Appendix A: Supported IPFIX Fields for Cisco Telemetry Broker

The table in this appendix contains a list of the IPFIX fields that Cisco Telemetry Broker supports.

Cisco Telemetry Broker extracts the numeric IDs (each numeric ID includes an Element ID and a PEN) from Information Elements within NetFlow messages and maps each of them to an associated descriptive name.



If Cisco Telemetry Broker doesn't recognize the numeric ID for an Information Element, the element information is still sent to Cisco Secure Cloud Analytics, but Cisco Telemetry Broker assigns a name to it using this format:

`unknownID_<ElementID>_<PEN>`

If you want to view the description for any element ID, see the [Cisco Secure Network Analytics Information Elements Guide](#).

ElementID	PEN	Name
1	0	octetDeltaCount
2	0	packetDeltaCount
3	0	deltaFlowCount
4	0	protocolIdentifier
5	0	ipClassOfService
6	0	tcpControlBits
7	0	sourceTransportPort
8	0	sourceIPv4Address
9	0	sourceIPv4PrefixLength
10	0	ingressInterface

ElementID	PEN	Name
11	0	destinationTransportPort
12	0	destinationIPv4Address
13	0	destinationIPv4PrefixLength
14	0	egressInterface
15	0	ipNextHopIPv4Address
16	0	bgpSourceAsNumber
17	0	bgpDestinationAsNumber
18	0	bgpNextHopIPv4Address
19	0	postMCastPacketDeltaCount
20	0	postMCastOctetDeltaCount
21	0	flowEndSysUpTime
22	0	flowStartSysUpTime
23	0	postOctetDeltaCount
24	0	postPacketDeltaCount
25	0	minimumIpTotalLength
26	0	maximumIpTotalLength
27	0	sourceIPv6Address
28	0	destinationIPv6Address
29	0	sourceIPv6PrefixLength
30	0	destinationIPv6PrefixLength

ElementID	PEN	Name
31	0	flowLabelIPv6
32	0	icmpTypeCodeIPv4
33	0	igmpType
34	0	samplingInterval
35	0	samplingAlgorithm
36	0	flowActiveTimeout
37	0	flowIdleTimeout
38	0	engineType
39	0	engineId
40	0	exportedOctetTotalCount
41	0	exportedMessageTotalCount
42	0	exportedFlowRecordTotalCount
43	0	ipv4RouterSc
44	0	sourceIPv4Prefix
45	0	destinationIPv4Prefix
46	0	mplsTopLabelType
47	0	mplsTopLabelIPv4Address
48	0	samplerId
49	0	samplerMode
50	0	samplerRandomInterval

ElementID	PEN	Name
51	0	classId
52	0	minimumTTL
53	0	maximumTTL
54	0	fragmentIdentification
55	0	postIpClassOfService
56	0	sourceMacAddress
57	0	postDestinationMacAddress
58	0	vlanId
59	0	postVlanId
60	0	ipVersion
61	0	flowDirection
62	0	ipNextHopIPv6Address
63	0	bgpNextHopIPv6Address
64	0	ipv6ExtensionHeaders
70	0	mplsTopLabelStackSection
71	0	mplsLabelStackSection2
72	0	mplsLabelStackSection3
73	0	mplsLabelStackSection4
74	0	mplsLabelStackSection5
75	0	mplsLabelStackSection6

ElementID	PEN	Name
76	0	mplsLabelStackSection7
77	0	mplsLabelStackSection8
78	0	mplsLabelStackSection9
79	0	mplsLabelStackSection10
80	0	destinationMacAddress
81	0	postSourceMacAddress
82	0	interfaceName
83	0	interfaceDescription
84	0	samplerName
85	0	octetTotalCount
86	0	packetTotalCount
87	0	flagsAndSamplerId
88	0	fragmentOffset
89	0	forwardingStatus
90	0	mplsVpnRouteDistinguisher
91	0	mplsTopLabelPrefixLength
92	0	srcTrafficIndex
93	0	dstTrafficIndex
94	0	applicationDescription
95	0	applicationId

ElementID	PEN	Name
96	0	applicationName
98	0	postIpDiffServCodePoint
99	0	multicastReplicationFactor
100	0	className
101	0	classificationEngineId
102	0	layer2packetSectionOffset
103	0	layer2packetSectionSize
104	0	layer2packetSectionData
128	0	bgpNextAdjacentAsNumber
129	0	bgpPrevAdjacentAsNumber
130	0	exporterIPv4Address
131	0	exporterIPv6Address
132	0	droppedOctetDeltaCount
133	0	droppedPacketDeltaCount
134	0	droppedOctetTotalCount
135	0	droppedPacketTotalCount
136	0	flowEndReason
137	0	commonPropertiesId
138	0	observationPointId
139	0	icmpTypeCodeIPv6

ElementID	PEN	Name
140	0	mplsTopLabelIPv6Address
141	0	lineCardId
142	0	portId
143	0	meteringProcessId
144	0	exportingProcessId
145	0	templateId
146	0	wlanChannelId
147	0	wlanSSID
148	0	flowId
149	0	observationDomainId
150	0	flowStartSeconds
151	0	flowEndSeconds
152	0	flowStartMilliseconds
153	0	flowEndMilliseconds
154	0	flowStartMicroseconds
155	0	flowEndMicroseconds
156	0	flowStartNanoseconds
157	0	flowEndNanoseconds
158	0	flowStartDeltaMicroseconds
159	0	flowEndDeltaMicroseconds

ElementID	PEN	Name
160	0	systemInitTimeMilliseconds
161	0	flowDurationMilliseconds
162	0	flowDurationMicroseconds
163	0	observedFlowTotalCount
164	0	ignoredPacketTotalCount
165	0	ignoredOctetTotalCount
166	0	notSentFlowTotalCount
167	0	notSentPacketTotalCount
168	0	notSentOctetTotalCount
169	0	destinationIPv6Prefix
170	0	sourceIPv6Prefix
171	0	postOctetTotalCount
172	0	postPacketTotalCount
173	0	flowKeyIndicator
174	0	postMCastPacketTotalCount
175	0	postMCastOctetTotalCount
176	0	icmpTypeIPv4
177	0	icmpCodeIPv4
178	0	icmpTypeIPv6
179	0	icmpCodeIPv6



ElementID	PEN	Name
180	0	udpSourcePort
181	0	udpDestinationPort
182	0	tcpSourcePort
183	0	tcpDestinationPort
184	0	tcpSequenceNumber
185	0	tcpAcknowledgementNumber
186	0	tcpWindowSize
187	0	tcpUrgentPointer
188	0	tcpHeaderLength
189	0	ipHeaderLength
190	0	totalLengthIPv4
191	0	payloadLengthIPv6
192	0	ipTTL
193	0	nextHeaderIPv6
194	0	mplsPayloadLength
195	0	ipDiffServCodePoint
196	0	ipPrecedence
197	0	fragmentFlags
198	0	octetDeltaSumOfSquares
199	0	octetTotalSumOfSquares

ElementID	PEN	Name
200	0	mplsTopLabelTTL
201	0	mplsLabelStackLength
202	0	mplsLabelStackDepth
203	0	mplsTopLabelExp
204	0	ipPayloadLength
205	0	udpMessageLength
206	0	isMulticast
207	0	ipv4IHL
208	0	ipv4Options
209	0	tcpOptions
210	0	paddingOctets
211	0	collectorIPv4Address
212	0	collectorIPv6Address
213	0	exportInterface
214	0	exportProtocolVersion
215	0	exportTransportProtocol
216	0	collectorTransportPort
217	0	exporterTransportPort
218	0	tcpSynTotalCount
219	0	tcpFinTotalCount

ElementID	PEN	Name
220	0	tcpRstTotalCount
221	0	tcpPshTotalCount
222	0	tcpAckTotalCount
223	0	tcpUrgTotalCount
224	0	ipTotalLength
225	0	postNATSourceIPv4Address
226	0	postNATDestinationIPv4Address
227	0	postNAPTSourceTransportPort
228	0	postNAPTDestinationTransportPort
229	0	natOriginatingAddressRealm
230	0	natEvent
231	0	initiatorOctets
232	0	responderOctets
233	0	firewallEvent
234	0	ingressVRFID
235	0	egressVRFID
236	0	VRFname
237	0	postMplsTopLabelExp
238	0	tcpWindowScale
239	0	biflowDirection

ElementID	PEN	Name
240	0	ethernetHeaderLength
241	0	ethernetPayloadLength
242	0	ethernetTotalLength
243	0	dot1qVlanId
244	0	dot1qPriority
245	0	dot1qCustomerVlanId
246	0	dot1qCustomerPriority
247	0	metroEvclid
248	0	metroEvcType
249	0	pseudoWireId
250	0	pseudoWireType
251	0	pseudoWireControlWord
252	0	ingressPhysicalInterface
253	0	egressPhysicalInterface
254	0	postDot1qVlanId
255	0	postDot1qCustomerVlanId
256	0	ethernetType
257	0	postIpPrecedence
258	0	collectionTimeMilliseconds
259	0	exportSctpStreamId

ElementID	PEN	Name
260	0	maxExportSeconds
261	0	maxFlowEndSeconds
262	0	messageMD5Checksum
263	0	messageScope
264	0	minExportSeconds
265	0	minFlowStartSeconds
266	0	opaqueOctets
267	0	sessionScope
268	0	maxFlowEndMicroseconds
269	0	maxFlowEndMilliseconds
270	0	maxFlowEndNanoseconds
271	0	minFlowStartMicroseconds
272	0	minFlowStartMilliseconds
273	0	minFlowStartNanoseconds
274	0	collectorCertificate
275	0	exporterCertificate
276	0	dataRecordsReliability
277	0	observationPointType
278	0	newConnectionDeltaCount
279	0	connectionSumDurationSeconds

ElementID	PEN	Name
280	0	connectionTransactionId
281	0	postNATSourceIPv6Address
282	0	postNATDestinationIPv6Address
283	0	natPoolId
284	0	natPoolName
285	0	anonymizationFlags
286	0	anonymizationTechnique
287	0	informationElementIndex
288	0	p2pTechnology
289	0	tunnelTechnology
290	0	encryptedTechnology
291	0	basicList
292	0	subTemplateList
293	0	subTemplateMultiList
294	0	bgpValidityState
295	0	IPSecSPI
296	0	greKey
297	0	natType
298	0	initiatorPackets
299	0	responderPackets

ElementID	PEN	Name
300	0	observationDomainName
301	0	selectionSequenceId
302	0	selectorId
303	0	informationElementId
304	0	selectorAlgorithm
305	0	samplingPacketInterval
306	0	samplingPacketSpace
307	0	samplingTimeInterval
308	0	samplingTimeSpace
309	0	samplingSize
310	0	samplingPopulation
311	0	samplingProbability
312	0	dataLinkFrameSize
313	0	ipHeaderPacketSection
314	0	ipPayloadPacketSection
315	0	dataLinkFrameSection
316	0	mplsLabelStackSection
317	0	mplsPayloadPacketSection
318	0	selectorIdTotalIPktsObserved
319	0	selectorIdTotalIPktsSelected

ElementID	PEN	Name
320	0	absoluteError
321	0	relativeError
322	0	observationTimeSeconds
323	0	observationTimeMilliseconds
324	0	observationTimeMicroseconds
325	0	observationTimeNanoseconds
326	0	digestHashValue
327	0	hashIPPayloadOffset
328	0	hashIPPayloadSize
329	0	hashOutputRangeMin
330	0	hashOutputRangeMax
331	0	hashSelectedRangeMin
332	0	hashSelectedRangeMax
333	0	hashDigestOutput
334	0	hashInitialiserValue
335	0	selectorName
336	0	upperCILimit
337	0	lowerCILimit
338	0	confidenceLevel
339	0	informationElementDataType



ElementID	PEN	Name
340	0	informationElementDescription
341	0	informationElementName
342	0	informationElementRangeBegin
343	0	informationElementRangeEnd
344	0	informationElementSemantics
345	0	informationElementUnits
346	0	privateEnterpriseNumber
347	0	virtualStationInterfaceId
348	0	virtualStationInterfaceName
349	0	virtualStationUUID
350	0	virtualStationName
351	0	layer2SegmentId
352	0	layer2OctetDeltaCount
353	0	layer2OctetTotalCount
354	0	ingressUnicastPacketTotalCount
355	0	ingressMulticastPacketTotalCount
356	0	ingressBroadcastPacketTotalCount
357	0	egressUnicastPacketTotalCount
358	0	egressBroadcastPacketTotalCount
359	0	monitoringIntervalStartMilliseconds

ElementID	PEN	Name
360	0	monitoringIntervalEndMilliseconds
361	0	portRangeStart
362	0	portRangeEnd
363	0	portRangeStepSize
364	0	portRangeNumPorts
365	0	staMacAddress
366	0	staIPv4Address
367	0	wtpMacAddress
368	0	ingressInterfaceType
369	0	egressInterfaceType
370	0	rtpSequenceNumber
371	0	userName
372	0	applicationCategoryName
373	0	applicationSubCategoryName
374	0	applicationGroupName
375	0	originalFlowsPresent
376	0	originalFlowsInitiated
377	0	originalFlowsCompleted
378	0	distinctCountOfSourceIPAddress
379	0	distinctCountOfDestinationIPAddress

ElementID	PEN	Name
380	0	distinctCountOfSourceIPv4Address
381	0	distinctCountOfDestinationIPv4Address
382	0	distinctCountOfSourceIPv6Address
383	0	distinctCountOfDestinationIPv6Address
384	0	valueDistributionMethod
385	0	rfc3550JitterMilliseconds
386	0	rfc3550JitterMicroseconds
387	0	rfc3550JitterNanoseconds
388	0	dot1qDEI
389	0	dot1qCustomerDEI
390	0	flowSelectorAlgorithm
391	0	flowSelectedOctetDeltaCount
392	0	flowSelectedPacketDeltaCount
393	0	flowSelectedFlowDeltaCount
394	0	selectorIDTotalFlowsObserved
395	0	selectorIDTotalFlowsSelected
396	0	samplingFlowInterval
397	0	samplingFlowSpacing
398	0	flowSamplingTimeInterval
399	0	flowSamplingTimeSpacing

ElementID	PEN	Name
400	0	hashFlowDomain
401	0	transportOctetDeltaCount
402	0	transportPacketDeltaCount
403	0	originalExporterIPv4Address
404	0	originalExporterIPv6Address
405	0	originalObservationDomainId
406	0	intermediateProcessId
407	0	ignoredDataRecordTotalCount
408	0	dataLinkFrameType
409	0	sectionOffset
410	0	sectionExportedOctets
411	0	dot1qServiceInstanceTag
412	0	dot1qServiceInstanceId
413	0	dot1qServiceInstancePriority
414	0	dot1qCustomerSourceMacAddress
415	0	dot1qCustomerDestinationMacAddress
417	0	postLayer2OctetDeltaCount
418	0	postMCastLayer2OctetDeltaCount
420	0	postLayer2OctetTotalCount
421	0	postMCastLayer2OctetTotalCount

ElementID	PEN	Name
422	0	minimumLayer2TotalLength
423	0	maximumLayer2TotalLength
424	0	droppedLayer2OctetDeltaCount
425	0	droppedLayer2OctetTotalCount
426	0	ignoredLayer2OctetTotalCount
427	0	notSentLayer2OctetTotalCount
428	0	layer2OctetDeltaSumOfSquares
429	0	layer2OctetTotalSumOfSquares
430	0	layer2FrameDeltaCount
431	0	layer2FrameTotalCount
432	0	pseudoWireDestinationIPv4Address
433	0	ignoredLayer2FrameTotalCount
434	0	mibObjectValueInteger
435	0	mibObjectValueOctetString
436	0	mibObjectValueOID
437	0	mibObjectValueBits
438	0	mibObjectValueIPAddress
439	0	mibObjectValueCounter
440	0	mibObjectValueGauge
441	0	mibObjectValueTimeTicks

ElementID	PEN	Name
442	0	mibObjectValueUnsigned
443	0	mibObjectValueTable
444	0	mibObjectValueRow
445	0	mibObjectIdentifier
446	0	mibSubIdentifier
447	0	mibIndexIndicator
448	0	mibCaptureTimeSemantics
449	0	mibContextEngineID
450	0	mibContextName
451	0	mibObjectName
452	0	mibObjectDescription
453	0	mibObjectSyntax
454	0	mibModuleName
455	0	mobileIMSI
456	0	mobileMSISDN
457	0	httpStatusCode
458	0	sourceTransportPortsLimit
459	0	httpRequestMethod
460	0	httpRequestHost
461	0	httpRequestTarget

ElementID	PEN	Name
462	0	httpMessageVersion
463	0	natInstanceID
464	0	internalAddressRealm
465	0	externalAddressRealm
466	0	natQuotaExceededEvent
467	0	natThresholdEvent
468	0	httpUserAgent
469	0	httpContentType
470	0	httpReasonPhrase
471	0	maxSessionEntries
472	0	maxBIBEntries
473	0	maxEntriesPerUser
474	0	maxSubscribers
475	0	maxFragmentsPendingReassembly
476	0	addressPoolHighThreshold
477	0	addressPoolLowThreshold
478	0	addressPortMappingHighThreshold
479	0	addressPortMappingLowThreshold
480	0	addressPortMappingPerUserHighThreshold
481	0	globalAddressMappingHighThreshold

ElementID	PEN	Name
482	0	vpnIdentifier
483	0	bgpCommunity
484	0	bgpSourceCommunityList
485	0	bgpDestinationCommunityList
486	0	bgpExtendedCommunity
487	0	bgpSourceExtendedCommunityList
488	0	bgpDestinationExtendedCommunityList
489	0	bgpLargeCommunity
490	0	bgpSourceLargeCommunityList
491	0	bgpDestinationLargeCommunityList
33002	0	ASAFirewallExtendedEvent
34000	0	TrustSecSourceIdentifier
34001	0	TrustSecDestinationIdentifier
34002	0	TrustSecSourceName
34003	0	TrustSecDestinationName
1232	9	SGTSourceId_9
1233	9	SGTDestinationId_9
9292	9	AVCRespsCountDelta_9
9303	9	AVCSumRespTime_9
9306	9	AVCSumServerRespTime_9



ElementID	PEN	Name
12172	9	ETAINitialDataPacket_9
12173	9	ETASequenceOfPacketLengthsAndTimes_9
12184	9	ETASequenceOfPacketLengths_9
12185	9	ETASequenceOfPacketTimes_9
12235	9	AVCSubApplicationValueIPFIX_9
12332	9	NVMUdid_9
12333	9	NVMLoggedInUser_9
12334	9	NVMOsName_9
12335	9	NVMOsVersion_9
12336	9	NVMSystemManufacturer_9
12337	9	NVMSystemType_9
12338	9	NVMProcessAccount_9
12339	9	NVMParentProcessAccount_9
12340	9	NVMProcessName_9
12341	9	NVMProcessHash_9
12342	9	NVMParentProcessName_9
12343	9	NVMParentProcessHash_9
12344	9	NVMDnsSuffix_9
12345	9	NVMDestinationHostname_9
12346	9	NVML4ByteCountIn_9

ElementID	PEN	Name
12347	9	NVML4ByteCountOut_9
12351	9	NVMOsEdition_9
12352	9	NVMModuleNameList_9
12353	9	NVMModuleHashList_9
12355	9	NVMInterfaceInfoUid_9
12356	9	NVMInterfaceIndex_9
12357	9	NVMInterfaceType_9
12358	9	NVMInterfaceName_9
12359	9	NVMInterfaceDetailsList_9
12360	9	NVMInterfaceMacAddress_9
12361	9	NVMUserAccountType_9
12362	9	NVMProcessAccountType_9
12363	9	NVMParentProcessAccountType_9
12364	9	NVMAgentVersion_9
12365	9	NVMProcessId_9
12366	9	NVMParentProcessId_9
12367	9	NVMProcessPath_9
12368	9	NVMParentProcessPath_9
12369	9	NVMProcessArgs_9
12370	9	NVMParentProcessArgs_9

ElementID	PEN	Name
12371	9	NVMFlowStartMsec_9
12372	9	NVMFlowEndMsec_9
12172	8712	FlowSensorEtaInitialDataPacket_8712
12173	8712	FlowSensorEtaSequenceOfPacketLengthsAndTimes_8712
29794	8712	FlowSensorInitiator_8712
29795	8712	FlowSensorTcpSynAckTotalCount_8712
29796	8712	FlowSensorTcpSrsTotalCount_8712
29797	8712	FlowSensorRoundTripTime_8712
29798	8712	FlowSensorServerResponseTime_8712
29799	8712	FlowSensorRetransmits_8712
29800	8712	FlowSensorTcpBadTotalCount_8712
29801	8712	FlowSensorTcpFragTotalCount_8712
29802	8712	FlowSensorSourceEmailIn_8712
29803	8712	FlowSensorSourceEmailOut_8712
29804	8712	FlowSensorSourceEmailInMess_8712
29805	8712	FlowSensorSourceEmailOutMess_8712
29806	8712	FlowSensorSourceEmailInTrys_8712
29807	8712	FlowSensorSourceEmailOutTrys_8712
29808	8712	FlowSensorDestinationEmailIn_8712

ElementID	PEN	Name
29809	8712	FlowSensorDestinationEmailOut_8712
29810	8712	FlowSensorDestinationEmailInMess_8712
29811	8712	FlowSensorDestinationEmailOutMess_8712
29812	8712	FlowSensorDestinationEmailInTrys_8712
29813	8712	FlowSensorDestinationEmailOutTrys_8712
29814	8712	FlowSensorTraces_8712
29817	8712	FlowSensorEmblcmpProtocol_8712
29818	8712	FlowSensorEmblcmpType_8712
29819	8712	FlowSensorEmblcmpCode_8712
29820	8712	FlowSensorApplicationIdentifier_8712
29821	8712	FlowSensorBadFlagXmas_8712
29822	8712	FlowSensorBadFlagSynFin_8712
29823	8712	FlowSensorBadFlagBadRst_8712
29824	8712	FlowSensorBadFlagNoAck_8712
29825	8712	FlowSensorBadFlagUrg_8712
29826	8712	FlowSensorBadFlagNoflag_8712
29828	8712	FlowSensorShortFragAttack_8712
29829	8712	FlowSensorFragPktTooShort_8712
29830	8712	FlowSensorFragPktTooLong_8712
29831	8712	FlowSensorFragDifferentSizes_8712

---

<b>ElementID</b>	<b>PEN</b>	<b>Name</b>
29832	8712	FlowSensorApplicationDetails_8712
29833	8712	FlowSensorSrcSgt_8712
56701	25461	PaloAltoApplicationIdentifier_25461
56702	25461	PaloAltoUserIdentifier_25461

## Appendix B: Supported Alerts

The following table contains the list of Cisco Telemetry Broker alerts.

Alert	Description
Appliance Disk Space Critically Low	The appliance's disk has less than 1G of free space. System operation is degraded.
Appliance Low Disk Space	This appliance's disk usage has reached 80% of its capacity.
Broker Node Dropping Packets	This node is dropping packets. Please make sure the broker node is not overloaded or misconfigured.
Broker Node Not Seen	This node has not communicated with the Manager for [x] minutes.
Config Validation Error	Config failed validation.
Destination Unreachable	This destination has sent a "destination unreachable" ICMP message.
Input Validation Error	Input failed validation.
Insufficient CPU Allocated	The recommended number of CPUs has not been allocated for this appliance.
Insufficient Memory Allocated	The recommended amount of memory has not been allocated for this appliance.
TLS Certificate Close to Expiration	The Manager's TLS certificate is about to expire. Please install a new certificate.
TLS Certificate Expired	The Manager's TLS certificate has expired. Please install a new certificate.

# Appendix C: Import UDP Director Configuration




Please note that importing UDP Director destination and rule configurations is optional.

## Export Your UDP Director Configuration

1. Log in to the UDP Director console as an **admin**.
2. Click the **Configuration** tab.
3. Click **Forwarding Rules**.
4. Choose **Export (Export the configuration file to local system)**.
5. Save the file to your workstation.

## Export Your UDP Director Configuration From a Manager

1. Log in to the Web App as **sysadmin**.
2. Click the  (**Global Settings**) icon.
3. From the drop-down menu, choose **UDP Director Configuration**.
4. Click the **Actions** menu.
5. Choose **Export Forwarding Rules**.
6. Click **Save**.

## Import Your UDP Director Configuration into Cisco Telemetry Broker

You can import your UDP Director Configuration only before you configure any destinations.

1. Log in to the Cisco Telemetry Broker Manager node.
2. Click the **Destinations** tab.
3. Click **Upload XML File**.
4. Choose the applicable file and click **Open**.

# Contact Support

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

- Contact your local Cisco Telemetry Broker Partner
- Contact Cisco Telemetry Broker 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](mailto: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

<b>Document Version</b>	<b>Published Date</b>	<b>Description</b>
1_0	March 14, 2024	Initial Version.
2_0	April 8, 2024	Deleted draft phrase from Data Flow page and replaced screenshot.

---

# 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)

