



Cisco Telemetry Broker

User Guide 2.3.3



Table of Contents

Introduction	10
Audience	10
Common Terms	10
Configure Accessibility Features	11
Common Abbreviations	11
Dashboard	12
How to Find This Page	12
View the Following Components	12
Inputs	12
Outputs	12
Broker Nodes	13
Alerts	13
CPU	14
Licensing	14
Telemetry Flows	15
Metrics	15
Explorer	16
How to Find This Page	16
Navigate the Tree View	17
Data Flow	19
How to Find This Page	19
View Snapshot Information in Input and Output Cards	19
View Data Flows	20
Input and Output Cards	20
Click vs. Hover	21
Alert and Status Icons	21
Filter Your Search	22
Filter	22

Clear Filters	22
Search	22
Import UDP Director Configuration	22
Inputs	23
View an Input	23
Add an Input	23
Edit an Input	23
Copy an Input	24
Via the Input Card	24
Drag and Drop	24
Delete an Input	24
Outputs	24
View a Output	24
Add a Output	24
Edit an Output	25
Delete an Output	25
Connections	25
Connect to an Output	25
Edit a Connection	25
Delete a Connection	26
Broker Nodes	27
How to Find This Page	27
View Broker Nodes	27
Sort Columns	27
Copy Numeric Strings	27
View Details of a Broker Node	28
Broker Node Details	28
How to Find This Page	28
View Details	28
Copy Numeric Strings	28

Configure HTTPS Proxy for Broker Nodes	28
Telemetry Interface	29
Monitor Interface	29
Edit a Broker Node	30
Remove a Broker Node	30
Back Up and Restore Inputs, Outputs, and Rules for a Broker Node	31
Metrics	32
Received Rate table	32
Compare to Capacity Toggle	32
Sent Rate table	32
Compare to Capacity Toggle	33
1-Minute Load Average table	33
Memory Usage table	33
Disk Storage table	33
Clusters	34
How to Find This Page	34
View Cluster Information	34
Sort Columns	34
Copy Numeric Strings	34
Add a Cluster	34
Edit a Cluster	35
Remove a Cluster	35
View Cluster Details	35
Cluster Details	35
How to Find This Page	35
View Cluster Details	36
Sort Columns	36
Copy Numeric Strings	36
Edit a Cluster's Configuration	36
Remove a Cluster	37

High Availability Clusters	37
Manager Node Details	39
How to Find This Page	39
View Details	39
Configure HTTPS Proxy for Manager Nodes	39
Metrics	40
1-Minute Load Average table	40
Memory Usage table	40
Disk Storage table	40
Alerts	41
Inputs	43
Rules for Adding, Editing, and Removing Inputs	44
How to Find This Page	44
Filter Your Search	44
Filter	44
Clear Filters	45
Search	45
Sort Columns	45
Import UDP Director Configuration	45
Add an Input	46
Disable Exporters Tracking	46
Copy an Input	47
Edit an Input	47
Remove an Input	47
View Details of an Input	48
Input Details	48
How to Find This Page	48
View Details	48
Copy Numeric Strings	49
More Details	49

Edit an Input	49
Disable Exporters Tracking	49
Copy an Input	50
Remove an Input	50
Connected Outputs	51
Create a Connection	51
Edit a Connection	52
Remove a Connection	52
Metrics	52
Exporters	52
Search	53
Filter	53
Add a Flow Generator Input	53
Enable Application Classification	53
Outputs	55
How to Find This Page	55
Import UDP Director Configuration	56
Filter Your Search	56
Filter	56
Clear Filters	57
Search	57
Sort Columns	57
Add an Output	57
Add a UDP Output	57
Reachability Check	58
Add a Cisco XDR Output	58
Locate the key and the URL	58
Add the Cisco XDR output	58
Edit an Output	59
Remove an Output	59

View Details of an Output	59
Output Details	59
How to Find This Page	60
View Details	60
Copy Numeric Strings	60
Edit an Output	60
Reachability Check	61
Remove an Output	61
Connected Inputs/Exporters	61
Filter the Table	62
Edit a Connection	62
Remove a Connection	62
Metrics: Sent Rate	62
Application Settings	64
General	64
Configure Inactivity Interval	64
Software Update	64
Upgrade Your Cisco Telemetry Broker Deployment	65
Download the Update File	65
Upload the Update File	65
Smart Licensing	66
Integrations	66
Software-Defined Application Visibility and Control	66
Enable SD-AVC Integration	67
User Management	68
Add a User	68
Edit a User	69
Remove a User	69
Change a User's Password	69
TLS Certificate	69

Upload TLS Certificate	69
Re-register Broker Nodes	70
Notifications	70
Syslog Notifications	70
Configure the Syslog Server	70
Enable the Syslog Server to Receive Notifications	71
Send a Test Syslog Notification	71
Severity and Facility Values	71
Email Notifications	72
Configure the SMTP Server	72
Enable a User to Receive Email Notifications	72
Send a Test Email Notification	72
Profile Settings	74
How to Find This Page	74
Edit Account Details	74
Change Your Password	74
Change the Cisco Telemetry Broker User Interface Theme	75
How to Find This Page	75
How Theme Preferences are Saved	75
Expand Cisco Telemetry Broker Manager and Broker Node Disk Size	76
1. Back Up the Partition Table Information	76
2. Delete All Existing VM Snapshots for the Appliance	76
3. Increase the Disk Size of the Appliance	77
4. Run ctb-part-resize.sh Script	77
5. Verify that Space has been Allocated	78
Shut Down or Reboot Cisco Telemetry Broker	79
Appendix A: Supported IPFIX Fields for Cisco Telemetry Broker	80
Appendix B: Supported Alerts	110
Appendix C: Import UDP Director Configuration	111
Export Your UDP Director Configuration	111

Export Your UDP Director Configuration From a Manager	111
Import Your UDP Director Configuration into Cisco Telemetry Broker	111
Appendix D: Differences in Types of Inputs and Outputs	112
Input Types	112
Output Types	114
Appendix E: AWS Configuration	116
Enable Flow Logging	116
Create an IAM User	116
Create the S3 Bucket Policy	117
Create a User Group	117
Replace S3 Bucket Code	117
Appendix F: Azure Configuration	119
Prerequisites	119
Enable Azure Flow Logs	119
Obtain Blob Service SAS URL	121
Register Azure Flow Log in Cisco Telemetry Broker	121
Appendix G: Proxy Log Input Configuration Guide	123
Web Proxy Server-side Requirements	123
IPFIX Templates	124
Configuration Parameters	126
Configure Your Own regex Patterns/Mappings	126
Regex Patterns and Field Transform Algorithms	127
Performance	129
Recommendations to achieve the best performance:	130
Appendix H: Flow Log Format Fields to IPFIX IE Mapping	131
Contact Support	136
Change History	137

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
Inputs	Ways in which Cisco Telemetry Broker collects or receives telemetry from a customer network. Cisco Telemetry Broker supports multiple types of inputs.
Outputs	Locations to which Cisco Telemetry Broker forwards telemetry. Cisco Telemetry Broker supports multiple types of outputs.
Destinations	External devices in the network outside of Cisco Telemetry Broker. Outputs send data to 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.
Connections	User-defined logic that tells Cisco Telemetry Broker how to forward telemetry from a single input to a single output.
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 export 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 outputs. 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:

Abbreviation	Description
DNS	Domain Name Server
GB	Gigabyte
HTTPS	Hypertext Transfer Protocol (Secure)
NAT	Network Address Translation
SSH	Secure Shell
UDPD	UDP Director
URL	Universal Resource Locator
VLAN	Virtual Local Area Network
VM	Virtual Machine

Dashboard

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

How to Find This Page

From the Cisco Telemetry Broker main menu on the left side of the page, choose **Dashboard**, 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 Output** 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

Outputs

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

- The number of outputs that have been configured in Cisco Telemetry Broker.
- The amount of telemetry sent to all outputs.
- The average daily rate of telemetry sent to all outputs. The average value is calculated from the last 30 days of telemetry.
- The number of outputs not accepting telemetry that is being sent to them (represented by the number in the Unreachable field). If any unreachable outputs exist, an alert icon is displayed next to the number. To see the list of unreachable outputs, hover over this icon.

- Each segment on the doughnut chart displays the amount of telemetry sent to each output. When you hover your cursor over a segment of this chart, you can view the following information:
 - the outputs name
 - the amount of telemetry sent to this specific outputs 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, an alert icon is displayed next to the node name. To see the list of all existing alerts for that broker node, hover over the alert icon.

Alerts

Alerts are messages that indicate that your system may not be working correctly or that you need to check an area on your system.

This component displays the number of unresolved (active) alerts grouped by severity. If there are no unresolved alerts, says there are no unresolved alerts. To open the Alerts page and see the full list of resolved and unresolved alerts, click **View all alerts**. See [Alerts](#) for more information. To manage the syslog notification settings, see [Notifications](#).

You can also see the recent alerts by clicking the bell (alert)  icon on the top right corner. The total count of unresolved alerts is displayed next to this icon. Clicking the icon opens a drop-down list of recent unresolved alerts, sorted by date. To open the Alerts page and see the full list of resolved and unresolved alerts, click **View all alerts**. See [Alerts](#) for more information.

CPU

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

- 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 30 days.

- The dotted dark gray line shows the average GB per day for the last 7 days. 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 outputs (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.
- Each input and output is shown in a different color on the chart.
- For Cisco XDR outputs, the telemetry statistics displayed here represent uncompressed data sent to Cisco XDR. Therefore, these statistics may be disproportionate to the actual telemetry sent (represented in the Outputs component).

Metrics

The charts in this section display the following data for the last 24 hours:

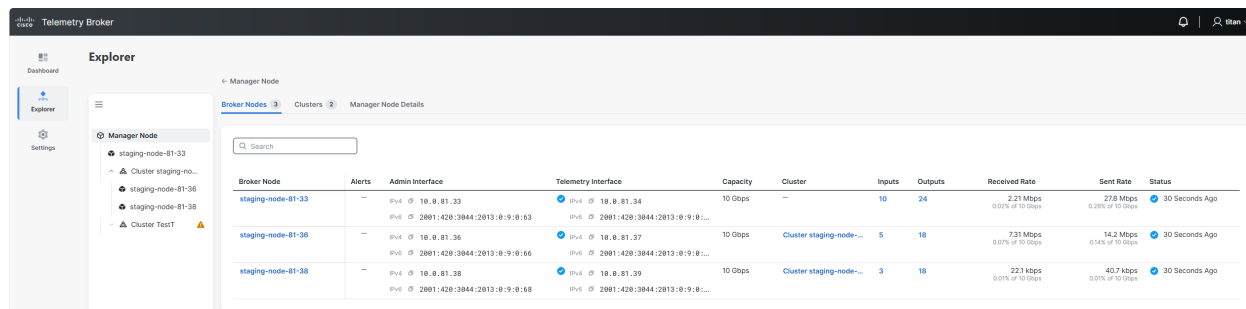
Total Received Rate The total amount of telemetry received from all inputs.

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

Explorer

After you choose **Explorer** from the main menu on the left side of the page, the Manager Node page opens by default, and the following tabs are displayed at the top of the page, with the Broker Nodes tab chosen by default:

- **Broker Nodes**
- **Clusters**
- **Manager Node Details**



When you choose a ...	The following tabs are displayed at the top of the page ...
broker node from the Tree View	<ul style="list-style-type: none"> • Data Flow • Inputs • Outputs • Broker Node Details
cluster from the Tree View	<ul style="list-style-type: none"> • Data Flow • Inputs • Outputs • Cluster Details

How to Find This Page

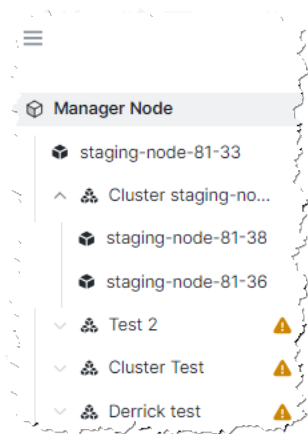
From the Cisco Telemetry Broker main menu on the left side of the page, choose **Explorer**.

Navigate the Tree View

On the left side of this page is the Tree View, a menu from which you can view information on several different pages (described in the sections below). The breadcrumbs near the top of this page shows you where you are in relation to the options you have chosen from this menu.

Use the  (**Tree View**) icon to toggle between closing and opening the Tree View.

Within the Tree View you can see the following hierarchy of information listed. Level 1 is at the top of the Tree View (Manager Node), and as you move down the list, each subsequent level (nested underneath its parent) is listed, ending in Level 3 entries at the bottom of the Tree View.



When you click this entry type from the Tree View...	This page opens...
<p>Level 1: Manager node</p>	<p>The Broker Nodes page with a list of all the broker nodes in your Cisco Telemetry Broker system.</p> <p>You can also choose from the following tabs from this view:</p> <ul style="list-style-type: none"> • Clusters Lists all the clusters in your Cisco Telemetry Broker system. • Manager Node Details Provides details about the Manager node.
<p>Level 2: A stand-alone</p>	<p>The Data Flow page, showing how the inputs assigned to</p>

When you click this entry type from the Tree View...	This page opens...
broker node or a cluster	<p>the entity you chose (stand-alone broker node or cluster) are connected to outputs.</p> <p>You can also choose from the following tabs from this view:</p> <ul style="list-style-type: none"> • Inputs Lists the inputs assigned to the entity (broker node or cluster) you chose. • Outputs Lists the outputs assigned to the entity (broker node or cluster). If the node is a part of a cluster, you can assign it only to the cluster and not directly to the node within the cluster. • Broker Node Details Provides details of the broker node (if you chose a broker node). • Cluster Details Provides details of the cluster you chose (if you chose a cluster).
<p>Level 3: A broker node contained within a particular cluster</p>	<p>The Data Flow page, showing how the inputs assigned to the broker node are connected to outputs.</p> <p>You can also choose from the following tabs from this view:</p> <ul style="list-style-type: none"> • Inputs Lists the inputs assigned to the broker node. • Outputs Lists the outputs assigned to the entity (broker node or cluster). If the node is a part of a cluster, you can assign it only to the cluster and not directly to the node within the cluster. • Broker Node Details Provides details of the broker node.

Data Flow

This page shows how the inputs are connected to the various outputs on a specific broker node, and allows you to add, update, or delete them. Note that in v2.2 and later, an input is local to a broker node or cluster. Adding, updating, or deleting an input on a broker node or cluster has no impact on any other broker node or cluster. This behavior is different from earlier versions where an input was shared among broker nodes and clusters, and you could choose to assign it to various broker nodes.

In v2.3 and later, what were previously called "destinations" are now known as "outputs." Outputs, like inputs, are now local to each broker node or cluster. This means that when a new output is added at the cluster level, it becomes available to all broker nodes within that cluster. However, if a broker node is part of a cluster, outputs can only be managed at the cluster level and not at the individual broker node level. If a broker node is added to a cluster, any outputs previously configured directly on that node will be removed and replaced by the cluster's outputs.

Also, during an upgrade to v2.3, any global destinations that are not assigned to an input will be removed. Only outputs that are connected to at least one input will be migrated.





How to Find This Page

1. From the Cisco Telemetry Broker main menu on the left side of the page, choose **Explorer**, then choose a broker node or cluster from the Tree View.
2. From the menu at the top of the page, choose **Data Flow**.

View Snapshot Information in Input and Output Cards

- Input or output status (indicated by a status icon). For more information, see [Alert and Status Icons](#).
- Type of input or output (represented by a unique icon). Hover over the icon to see entity type.

- Input or output name.
- Any applicable alert (indicated by an alert icon). For more information, see [Alert and Status Icons](#).
- The total data received (for inputs) or sent (for outputs) for the last 24 hours.
- The number of inputs or outputs for a particular entity.
 - (Input card) The number of outputs to which the input is connected, represented by the number on the right edge of each card (). If a **Plus** icon is displayed, this indicates that the input has no connected outputs.
 - (Output card) The number of inputs to which the output is assigned, represented by the number on the left edge of each card ().

View Data Flows



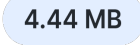
Input and Output Cards

Each input and output is represented by a card on the left and right sides of the page, respectively. Each card displays the following information.

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

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

You can click a connection between an input and an output to see the following information:

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

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 card	<ul style="list-style-type: none"> • Border of the card turns blue. • Data flow lines for that input or output turn dark blue. All other lines on the Data Flow page remain light blue.
Click a card	<ul style="list-style-type: none"> • Border of the card turns blue. • Data flow lines for that input or output turn dark blue. All other lines on the Data Flow page remain gray.



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

Alert and Status Icons


Alerts are messages that indicate that your system may not be working correctly or that you need to check an area on your system. Alerts marked by a red critical icon or an orange warning icon are still active. Refer to the following table for more information about these icons.


Alert Type	Definition
Critical 	Indicates an exceptional condition impacting system functionality. System operation is degraded. Refer to Appendix B for the complete list of alerts.
Warning 	Indicates a part of the system is misconfigured and/or is not working correctly. Overall system health is not impacted. Refer to Appendix B for the complete list of alerts.

To view the description for an existing alert or status icons for a specific input or output, hover your cursor over the associated icon. Refer to the following table for the various descriptions. For a list of Cisco Telemetry Broker alerts, see [Appendix B: Supported Alerts](#).

Filter Your Search

Filter

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

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

Either the Filter Inputs or Filter Outputs 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 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 output (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 as well as create multiple outputs with the same name. So if you search for an input or output for which there are more than one with the same name, 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 output 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 output on a broker node or cluster, 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, outputs, and rules.

Inputs

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

- If a **Plus** icon is displayed, this indicates that the input has no connected outputs.
- The **Connected Output** icon displays the number of outputs to which the input is connected. When you hover over it, it changes to the **Plus** icon.
- To view details for an input, on the applicable card, click the  (**Ellipsis**) icon > **View Input**.


View an Input

On the applicable card, click the  (**Ellipsis**) icon > **View Input**.

Add an Input

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.

Edit an Input

1. Click the Input name within the applicable card, or, on the applicable card, click the  (**Ellipsis**) icon > **Edit Input**.
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**.

Copy an Input

To copy an input to a broker node or cluster, complete either of the following procedures.

Via the Input Card

1. On the applicable input card, click the **⋮ (Ellipsis)** icon > **Copy Input**.

The Copy Input dialog opens.

2. Configure all applicable fields and click **Save**.

Drag and Drop

1. Hold the left-click button on your mouse and drag the input card over the top of the applicable broker node listed in the menu on the left.

When you release the left-click button, the Copy Input dialog opens.

2. Configure all applicable fields and click **Save**.

Delete an Input

1. On the applicable input card, click the **⋮ (Ellipsis)** icon > **Delete Input**.
2. In the Remove Input dialog, click **Remove**.

Outputs

On the left edge of each card, the **12 (Connected Inputs)** icon is displayed. This icon represents the number of inputs to which the output is connected

View a Output

On the applicable output card, click the **⋮ (Ellipsis)** icon > **View Output**.

Add a Output

1. Click **Add Output** in the upper right corner of the Outputs list.

The Add Output panel opens.

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

The second Add Output dialog opens.

3. Complete the applicable fields and click **+ Add Output**.

The new output card is now displayed in the Output list on the Data Flow page.

Edit an Output

1. On the applicable card, click the **⋮ (Ellipsis)** icon > **Edit Output**.

The Edit Output panel opens.

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



(View Details) icon .

3. Click **Save**.

Delete an Output

On the applicable card, click the **⋮ (Ellipsis)** icon > **Delete Output**.

Connections

Connect to an Output

Do one of the following:

Drag and drop the applicable input card onto the applicable output card.

OR

1. On the applicable input card, click the **⋮ (Ellipsis)** icon > **Connect to an Output**.


The Connect to an Output dialog opens.

2. Complete all applicable fields 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 output 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 output, 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 output, then click the  (**Remove**) icon.

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

Broker Nodes

The Cisco Telemetry Broker Nodes page displays a list of all of your broker nodes.

How to Find This Page

1. From the Cisco Telemetry Broker main menu on the left side of the page, choose **Explorer**.

The Manager Node option in the Tree View is enabled by default.

2. From the menu at the top of the page, choose **Broker Nodes**. Note that the number beside the Broker Nodes tab heading represents the total number of broker nodes.

View Broker Nodes

You can view the following information on this page:

- Broker node name
- Associated alerts
- 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)
- The number of inputs per node
- Received and Sent rate in bps
- Status of the broker node and the last time the Manager node communicated with it

As you start to type your entry in the Search field, the table dynamically filters to display a list of entries that contain the characters you have entered.

Sort Columns

Where applicable, use the ▲ (**Move Up**) icon and the ▼ (**Move Down**) icon at the top of a column to reverse the sort order of the column. Note that you must first click the column name before you can view the icons.

Copy Numeric Strings

Click the  (**Copy**) icon to copy numeric strings such as IP addresses and subnet masks.

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 column. For information about this page, see the next section, [Broker Node Details](#).

Broker Node Details

On this page you can view details about a particular broker node.

How to Find This Page

1. From the Cisco Telemetry Broker main menu on the left side of the page, choose **Explorer**.
2. Choose a broker node from the Tree View, then choose **Broker Node Details** from the menu at the top of the page.

OR

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

View Details

Across the top of the page you can view the following information:

- Hostname and Admin interface (Management Network) IPv4/IPv6 addresses
- Status of the input and the last time it received telemetry
- Associated alerts
- Received rate (in bytes per second) for the last 24 hours
- Sent rate (in bytes per second) for the last 24 hours

Copy Numeric Strings

Click the  (**Copy**) icon to copy numeric strings such as IP addresses and subnet masks.



Configure HTTPS Proxy for Broker Nodes

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

From v2.3 and later, you can now configure HTTPS Proxy settings individually for each broker node and manager node. You can enable or disable the proxy per node as needed.

This replaces the previous system-wide (global) proxy configuration, allowing greater flexibility for deployments where broker and manager nodes are in different subnets or environments that require separate proxy settings.

i Cisco Telemetry Broker does not support using HTTP proxy servers.

1. In the General section of **Broker Node Details**, click the  (**Edit**) icon next to **HTTPS Proxy**.
2. Enable the **Use HTTPS Proxy** toggle ()
3. Enter an **IP Address** and **Port**.
4. Click **Save**.

i If you are upgrading from v2.2.1 and had a global proxy configured and enabled, all broker nodes will automatically inherit this proxy setting after the upgrade.

i If the global proxy was disabled before upgrading, proxy settings will remain disabled for all broker nodes unless you enable them individually after the upgrade.

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 outputs 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 Outputs and Inputs pages).

Note the following parameters 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 **Remove Broker Node**.
2. In the Remove dialog, click **Remove**.

Back Up and Restore Inputs, Outputs, and Rules for a Broker Node

If you want to back up inputs, outputs, and rules for an existing broker node, use the backup and restore options.

You might want to do this in the following scenarios:

- You want to remove a broker node but save its existing inputs, outputs, and rules.
- You want to copy the existing inputs, outputs, and rules of a broker node to a new broker node.

The process is as follows:

1. Complete a backup of the existing broker node's inputs, outputs, and rules. On the Broker Nodes Details page of the broker node whose inputs, outputs, and rules you want to back up, click **Backup Rules**.
2. Restore the inputs, outputs, and rules of the broker node from Step 1 to the new broker node. On the Broker Nodes Details page of the new broker node, click **Restore Rules**.

Note the following parameters:

- All existing inputs, rules, outputs, and proxy settings are overwritten by the restoration file.
- All outputs are added to the restoration file except the Cisco XDR output.
- From v2.3 and later, you can back up a broker node's inputs, outputs, and rules from one Cisco Telemetry Broker deployment and restore them to another deployment, provided both are on the same version.
- You cannot back up or restore inputs and outputs that require a password.
- You cannot back up and restore broker nodes that are part of a cluster. You can only back up and restore standalone broker nodes.

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 output.

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 24 hours
- Last 7 days
- Last 30 days



Received Rate table

This table shows telemetry that this broker node has received over time.

Use the  (**Filter**) icon to filter the telemetry by the following parameters. You can choose more than one option within each filter.


- Per Input
- Per Exporter

Compare to Capacity Toggle



- 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.

Sent Rate table

This table shows telemetry that this broker node has sent over time.

Use the  (**Filter**) icon to filter the telemetry per output. You can choose more than one output within the filter.

Compare to Capacity Toggle

- 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 output(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.

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 Metrics section.) 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 Metrics section.) 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 Metrics section.) 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.

Clusters

The Clusters page lists the clusters configured for your Cisco Telemetry Broker system.

How to Find This Page

1. From the Cisco Telemetry Broker main menu on the left side of the page, choose **Explorer**.

The Manager Node option in the Tree View is enabled by default.

2. From the menu at the top of the page, choose **Clusters**. Note that the number beside the Clusters tab heading represents the total number of clusters.

View Cluster Information

You can view the following information on this page:

- Cluster name
- Virtual IP addresses
- The number of broker node assigned to the cluster
- The number of inputs assigned to the cluster
- Actions (edit or remove a cluster)

Sort Columns

Where applicable, use the ▲ (**Move Up**) icon and the ▼ (**Move Down**) icon at the top of a column to reverse the sort order of the column. Note that you must first click the column name before you can view the icons.

Copy Numeric Strings

Click the  (**Copy**) icon to copy numeric strings such as IP addresses and subnet masks.

Add a Cluster

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

The Add Cluster dialog opens.

2. Configure all applicable information.
3. Click **Add Cluster**.

A Confirm dialog opens that lists important information to be aware of before confirming your edits.

4. If you want to finalize your edits, click **Confirm**. Otherwise, click **Cancel**.



- It can take up to 3 minutes for the configuration to propagate and for the VIP addresses to become available on your network.


Edit a Cluster

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

The Edit Cluster dialog opens.

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

Remove a Cluster

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

The Remove Cluster dialog opens.

2. Click **Remove**.

View Cluster Details

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

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

Cluster Details

The Cluster Details page lists the details of all clusters configured for your Cisco Telemetry Broker system.

How to Find This Page

1. From the Cisco Telemetry Broker main menu on the left side of the page, choose **Explorer**.
2. Choose a cluster from the Tree View, then choose **Cluster Details** from the menu at the top of the page.

OR

On the Clusters page, in the Clusters table, click the applicable cluster name in the Cluster column.

View Cluster Details

You can view the following data on this page:

- Cluster name
- IPv4 address and IPv6 address
- A list of the broker nodes that belong to the cluster, along with the following related details for each broker node:
 - Broker node name
 - Associated alerts
 - Admin interface
 - Telemetry interface
 - Capacity of the broker node
 - Number of inputs assigned to the broker node
 - Received Rate
 - Sent Rate
 - Status

To view the Broker Node Details page for a broker node, click a broker node name in the List of Broker Nodes table.


Sort Columns

Where applicable, use the ▲ (**Move Up**) icon and the ▼ (**Move Down**) icon at the top of a column to reverse the sort order of the column. Note that you must first click the column name before you can view the icons.

Copy Numeric Strings

Click the  (**Copy**) icon to copy numeric strings such as IP addresses and subnet masks.

Edit a Cluster's Configuration

1. In the appropriate cluster section, click the  (**Edit**) icon .

The Edit Cluster dialog opens.

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

A Confirm dialog opens that lists important information to be aware of before confirming your edits.

3. If you want to finalize your edits, click **Confirm**. Otherwise, click **Cancel**.

Remove a Cluster

1. In the appropriate cluster section, click the  (**Remove**) icon.

The Remove Cluster dialog opens.

2. Click **Remove**.

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

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 outputs.

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 assign a broker node to a cluster, the UDP and Proxy Log inputs are deleted.
- 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 address, a virtual IPv6 address, or both, to a cluster. Note the following guidelines:
 - If assigning a virtual IPv4 address, in each broker node's telemetry interface you must have configured the IPv4 address in the same subnet of the virtual IPv4 address.
 - If assigning a virtual IPv6 address, in each broker node's telemetry interface you must have configured the IPv6 address in the same subnet of the virtual IPv6 address.

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](#).

Manager Node Details

The Cisco Telemetry Broker Manager Node Details page shows details and metrics for your Cisco Telemetry Broker Manager.

How to Find This Page

1. From the Cisco Telemetry Broker main menu on the left side of the page, choose **Explorer**.

The Manager Node option in the Tree View is enabled by default.

2. From the menu at the top of the page, choose **Manager Node Details**.

View Details

Across the top of the page you can view the following information:

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



Configure HTTPS Proxy for Manager Nodes

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

From v2.3 and later, you can now configure HTTPS Proxy settings individually for each broker node and manager node. You can enable or disable the proxy per node as needed.

This replaces the previous system-wide (global) proxy configuration, allowing greater flexibility for deployments where broker and manager nodes are in different subnets or environments that require separate proxy settings.

 Cisco Telemetry Broker does not support using HTTP proxy servers.

1. In the General section of **Manager Node Details**, click the  (**Edit**) Icon next to **HTTPS Proxy**.
2. Enable the **Use HTTPS Proxy** toggle ()
3. Enter an **IP Address** and **Port**.
4. Click **Save**.



The manager node proxy must be configured separately after the upgrade from an earlier version.

Metrics

Details of the Metrics information are described below.

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 Metrics section.) 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 Metrics section.) 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 Metrics section.) 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 24 hours
- Last 7 days
- Last 30 days

Alerts

This page contains a list of all resolved and unresolved alerts. Alerts are messages that indicate that your system may not be working correctly or that you need to check an area on your system.

Alerts marked by a red critical icon or an orange warning icon are still active. Refer to the following table for more information about these icons.

Alert Type	Definition
Critical 	Indicates an exceptional condition impacting system functionality. System operation is degraded. Refer to Appendix B for the complete list of alerts.
Warning 	Indicates a part of the system is misconfigured and/or is not working correctly. Overall system health is not impacted. Refer to Appendix B for the complete list of alerts.

Alerts that have been resolved are marked with a white check mark in a blue circle. The list begins with the newest alert at the top and ends with the oldest alert at the bottom.

The following parameters apply to this page:

- By default, this page lists all the resolved and unresolved alerts. The number of all alerts that have occurred is displayed on the **All** button at the top of this component.
- Click the **Unresolved** button to filter the list by this category. The number of unresolved alerts is displayed on the **Unresolved** button at the top of this component.
- To filter by additional options, use the **Most Recent on Top** drop-down list.
- Alert entries contain the following information:
 - Alert name.
 - Associated broker node or output. Click its link to open the Broker Node Details page for a broker node or the Output Details page for an output. Some alerts might also contain the associated input. If you click this link, the Inputs page for that input opens.
 - The date and time the alert began. Resolved alerts also display the date and time it was resolved.

-
- To view more alerts, click the **See more...** link at the bottom of the page.

To view the Cisco Telemetry Broker Documents page, click the **Documentation** button located in the upper right corner. You can also access these documents by clicking [here](#).

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. For information about how to enable a virtual broker node to receive telemetry from a Flow Generator input, as well as how to add more CPUs, memory, and a network interface to a broker node, refer to the [Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide](#).

- 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 on one node and then copy the input to all broker nodes.
- If you want to process VPC Flow Log telemetry, you should create a VPC Flow Log input.
- If you want to process Azure Flow Log telemetry, you should create an Azure Flow Log input.
- 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 and create a Flow Generator input.
- If you want to generate IPFIX records based on log messages from a web proxy server, you should create a proxy log input. Note: the log messages will be parsed based on regex patterns. Examples patterns are provided, but you can create a new pattern (see 'Configure Your Own regex Patterns/Mappings' in [Appendix G: Proxy Log Input Configuration Guide](#).)

You can forward telemetry from a Flow Generator input to Cisco XDR or UDP IPv4 and IPv6 outputs.

The Flow Generator sends IPFIX records over IPv4 if only an IPv4 address is assigned to the telemetry interface of the broker node, and over IPv6 if only an IPv6 address is assigned to the telemetry interface of the broker node.



When a broker node telemetry interface is in dual stack mode (assigned both IPv4 and IPv6 addresses) and you enable the **Prefer IPv6 over IPv4** option in the **Add Input** panel for a Flow Generator input, the Flow Generator will use IPv6 to send IPFIX records; otherwise, it will use IPv4.



Note that if your system is receiving IPv4 from an input, it can forward IPFIX to only IPv4 outputs. If your system is receiving IPv6 from an input, it can forward IPFIX to only IPv6 outputs.

Rules for Adding, Editing, and Removing Inputs

- To begin collecting telemetry on a broker node or cluster, you need to create one or more inputs for that node or cluster.
- When you remove a cluster or node from the Manager node, all inputs assigned to that cluster or node are removed.

How to Find This Page

1. From the Cisco Telemetry Broker main menu on the left side of the page, choose **Explorer**.
2. Choose a broker node or cluster from the Tree View, then choose **Inputs** from the menu at the top of the page. Note that the number beside the Inputs tab heading represents the total number of inputs.

You can see the following information on the Inputs page:

- Status.
- Input type.
- Input name.
- Associated alerts.
- Assigned outputs. (To see the list of the outputs 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.
- Actions (copy, edit, or remove an input).

Filter Your Search

Filter

1. Click  **Filter**.


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**.
3. (Conditional) If you want to reset all filters, 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.
- To clear one or more filter fields, click  **Filter** (which contains the number of filters applied). When the Filter Inputs panel opens, make your changes and click **Apply**.

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.

Sort Columns

Where applicable, use the ▲ (**Move Up**) icon and the ▼ (**Move Down**) icon at the top of a column to reverse the sort order of the column. Note that you must first click the column name before you can view the icons.

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 output, 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, outputs, and rules.

Add an Input

Please note that there are some restrictions when assigning an input to a node:

- All input types can be assigned to nodes that are not part of clusters.
- HA compatible inputs (UDP and Proxy Log) can be assigned to clusters, but they cannot be assigned to nodes that are part of a cluster.
- Inputs which are not HA compatible (VPC/Azure Flow Log and Flow Generator) can be assigned to nodes that are part of a cluster, but they cannot be assigned to clusters.

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. For information about the Disable Exporters Tracking toggle, see [Disable Exporters Tracking](#).

4. When finished, click **Add Input**.

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.

Copy an Input

1. In the Actions column for the applicable input, click the  (**Copy**) icon.

The Copy Input dialog opens.

2. Configure all applicable fields and click **Save**.

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 Outputs 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](#).

Input Details

On this page you can view more detailed information about a particular input.

How to Find This Page

1. From the Cisco Telemetry Broker main menu on the left side of the page, choose **Explorer**.
2. Choose a broker node or cluster from the Tree View, then choose **Inputs** from the menu at the top of the page. Note that the number beside the Inputs tab heading represents the total number of inputs.
3. In the Inputs List table, click an input in the Input Name column.

View Details

Across the top of the page you can view the following information, depending on the input type:

- Input type.
- Status.
- Broker node that the input is assigned to. To access the Broker Node Details page for the assigned broker node, click its name.
- Associated alerts.

- 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.


Copy Numeric Strings

Click the  (**Copy**) icon to copy numeric strings such as IP addresses and subnet masks.

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. For information about the Disable Exporters Tracking toggle, see [Disable Exporters Tracking](#).
3. When finished, click **Save**.

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.

Copy an Input

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

The Copy Input dialog opens.

2. Configure all applicable fields and 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 Outputs 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 Outputs

Where applicable, use the ▲ (**Move Up**) icon and the ▼ (**Move Down**) icon at the top of a column to reverse the sort order of the column. Note that you must first click the column name before you can view the icons.

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

- Total number of outputs connected to this input. (This number is displayed after the "Connected Outputs" title.)
- Status.
- Output type.
- Output name of the connection output.
- Associated alerts.
- The amount of telemetry sent to this output for the last 24 hours.
- The rate of telemetry sent to this output for the last 24 hours.
- Actions (edit or remove a connection).

Create a Connection

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

1. In the upper right corner of the table, click + **Connect to**.

The Connect to an Output panel opens.

2. Choose the output.
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 output. Only traffic coming from exporter IPs within the specified subnet will be forwarded. Enter the subnets over which this output 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 output 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 output 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 Output 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 7 days
- Last 30 days

Use the  (**Filter**) icon to filter the telemetry per exporter. You can choose more than one exporter within the filter.

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 outputs.
- 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.

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.

Enable Application Classification

The Flow Generator input now offers improved application classification features and integration with Cisco's Software-Defined Application Visibility and Control (SD-AVC) Cloud. With these enhancements, broker nodes can analyze network traffic using the Next Generation Network-Based Application Recognition (NBAR2) Deep Packet Inspection engine for accurate application identification. Additionally, integration with the SD-AVC Cloud allows broker nodes to automatically receive dynamic updates to the protocol pack used by the application classifier.

When these settings are enabled, the broker node analyzes traffic and appends application identification information to the generated NetFlow. This enables application-level telemetry and enhances visibility into network activity. This setting is disabled by default.

The NBAR2-based Deep Packet Inspection engine can receive dynamic updates from cloud-based Software-Defined Application Visibility and Classification (SD-AVC) service.



Application Classification can be enabled independently of cloud integration, but dynamic updates require SD-AVC integration to be enabled. For more information, see [Integrations](#).

Outputs

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

- **UDP Outputs** A output that receives UDP data at a specific IP address and port.
- **Cisco XDR Outputs** A output that points data to a customer-owned Cisco XDR Analytics account.

Configuring a Cisco XDR output 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 XDR Analytics.



Cisco Telemetry Broker supports only one Cisco XDR output per Cisco Telemetry Broker system.

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

- 80K FPS per virtual broker node when it is solely dedicated to uploading data to a Cisco XDR output. This requires a configuration with a single UDP input, forwarding to one Cisco XDR output, with no additional inputs or outputs. The virtual broker node must also be provisioned with 8 reserved CPUs, 8 cores per socket, and 12 GB of RAM.
- 300K FPS per broker node for a hardware deployment (M6).


How to Find This Page

1. From the Cisco Telemetry Broker main menu on the left side of the page, choose **Explorer**.
2. Choose a broker node or cluster from the Tree View, then choose **Outputs** from the menu at the top of the page. Note that the number beside the Outputs tab heading represents the number of outputs per node or cluster.

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

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

You can see the following information on the Outputs page:

- Status.
- Output type.
- Output name.
- Associated alerts.
- Assigned inputs. (To see the list of inputs assigned to an output, click the  **(Information)** icon.)
- The amount of telemetry sent to each output for the last 24 hours.
- The combined rate of telemetry sent to each output for the last 24 hours.

Import UDP Director Configuration

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



Once you have created your first output on a broker node or cluster, 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, outputs, and rules.

Filter Your Search

Filter

1. Click  **Filter**.


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**.
3. (Conditional) If you want to reset all filters, 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.
- To clear one or more filter fields, click  **Filter** (which contains the number of filters applied). When the Filter Inputs panel opens, make your changes and click **Apply**.

Search

In the Search field, type the name of the output 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 outputs with the same name. So if you search for a output for which there are more than one with the same name, all matching entries will be displayed after your search has finished processing.

Sort Columns

Where applicable, use the ▲ (**Move Up**) icon and the ▼ (**Move Down**) icon at the top of a column to reverse the sort order of the column. Note that you must first click the column name before you can view the icons.

Add an Output

Add a UDP Output

1. In the upper right corner of the page, click **+ Add Output**.
The Add Output panel opens.
2. Enter or select a output type and click **Next**.
3. Configure all applicable fields. If you want to be alerted of outputs 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."
4. When finished, click **Add Output**.



- The Reachability Check feature is available only for non-Cisco XDR Analytics outputs.
- You can disable this feature on a per output basis.

- Disable this feature if your output 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.

Add a Cisco XDR Output



- In Cisco Telemetry Broker, you can add only 1 Cisco XDR Output per node or cluster.
- Cisco Telemetry Broker extracts flow data from NetFlow V5, NetFlow V9, and IPFIX packets, and sends this data to XDR Analytics.
- If your Cisco Telemetry Broker deployment contains light telemetry, it may take up to 20 minutes for telemetry to appear on the Outputs page after you add an Cisco XDR output.

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

Locate the key and the URL

1. Log in to Cisco XDR 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 Cisco XDR output

1. Log in to Cisco Telemetry Broker.
2. In the upper right corner of the page, click **Add Output > SCA (XDR) Output**.
3. Enter an output **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 Cisco XDR as a Cisco Telemetry Broker output, you should be able to see telemetry from Cisco Telemetry Broker in the XDR Analytics Event Viewer within 30 minutes. If you do not, please contact swatchc-support@cisco.com with your portal URL for assistance.


Edit an Output

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

Remove an Output

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

To remove a output, complete the following steps:

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

View Details of an Output

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

Output Details

On this page you can view more detailed information about a particular output.

How to Find This Page

1. From the Cisco Telemetry Broker main menu on the left side of the page, choose **Explorer**.
2. Choose a broker node or cluster from the Tree View, then choose **Outputs** from the menu at the top of the page. Note that the number beside the Outputs tab heading represents the total number of outputs.
3. In the Outputs List table, click a output in the Output Name column.

View Details

Across the top of the page you can view the following information, depending on the output type:

- Output type
- Status
- Node to which it is assigned to
- Associated alerts
- The amount of telemetry sent to this output from the associated input for the last 24 hours
- The rate of telemetry sent to this output from the associated input for the last 24 hours





For Cisco XDR output only: Statistics displayed in the Sent Rate section are transformed and compressed data. The Sent Last and Sent Rate statistics in the Connected Inputs/Exporters section are original data (before being transformed and compressed).

Copy Numeric Strings

Click the  (**Copy**) icon to copy numeric strings such as IP addresses and subnet masks.

Edit an Output

1. In the upper right corner of the page, click  **Edit Output**.
The Edit Output panel opens.
2. Make your changes. 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."

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

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](#).

Remove an Output

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

To remove a output, complete the following steps:

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

The Remove Output 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 output, and the second number represents the total number of exporters assigned to all inputs that are assigned to this output.

Where applicable, use the ▲ (**Move Up**) icon and the ▼ (**Move Down**) icon at the top of a column to reverse the sort order of the column. Note that you must first click the column name before you can view the icons.

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


- Status.
- Input type.


- Input name.
- Number of exporters sending data to a particular input.
- The amount of telemetry sent from the input for the last 24 hours.
- The rate of telemetry sent from the input for the last 24 hours.
- Actions (Edit or remove a connection).

Filter the Table


- Click **All** to see a list of all the inputs that are connected to this output. The number in parentheses in the All button represents the total number of inputs assigned to this output, 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.

Edit a Connection

 You can only edit connections to a output 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 output 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 Output panel opens.
2. Make your edits and click **Save**.

Remove a Connection


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

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 output 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 7 days
- Last 30 days

Use the  (**Filter**) icon to filter the telemetry by the following parameters. You can choose more than one option within each filter.

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



For Cisco XDR outputs, you can filter the telemetry in this table only per broker node or per the total amount received.

Application Settings

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

General

Software Update

Smart Licensing

User Management

TLS Certificate

Notifications

General

From the Cisco Telemetry Broker main menu on the left side of the page, choose **Settings**.

*The Settings page opens. The **General** tab is selected by default.*

Configure Inactivity Interval

The Inactivity Interval configuration allows you to configure the amount of time before Cisco Telemetry Broker marks a telemetry input or an output as inactive. For an input, this indicates that no telemetry has been received for the configured time frame, and for an output, that no telemetry has been sent for the configured time frame.

1. In the Inactivity Interval section, choose an **Inactivity Interval** in minutes from the Inactivity Interval drop-down list.
2. 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 outputs.

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 the latest version to ensure a successful upgrade. For more information, refer to the latest version of the Release Notes.


1. Click the  (**Settings**) icon.
The Application Settings page opens.
2. Click the **Software Update** tab. The number 1 is displayed beside this menu option when a newer version of software is available.

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 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.

Using the Actions button in the upper right corner of the page, you can do any of the following:

- Renew Authorization Now
- Renew Registration Now
- Reregister
- Deregister

To view or edit transport settings, click **View/Edit** in the Transport Settings field.

Integrations

Software-Defined Application Visibility and Control

Cisco Telemetry Broker can now be integrated with Software-Defined Application Visibility and Control (SD-AVC). SD-AVC is a cloud-based service providing dynamic updates to the Next Generation Network-Based Application Recognition (NBAR2) based Deep Packet Inspection (DPI) engine, improving detection accuracy and coverage as new application signatures become available.

The NBAR2-based DPI engine running on broker nodes can dynamically download updates from the SD-AVC cloud service. This cloud integration allows Cisco Telemetry Broker to leverage the latest application signatures and analysis techniques as they become available.

For this integration to work, Cisco Smart Software Licensing must be set up first. Once Smart Licensing is enabled and the device is **Registered**, you can enable SD-AVC integration in Cisco Telemetry Broker. SD-AVC integration cannot be enabled when the Cisco Telemetry Broker system is not Registered to a Smart Account. SD-AVC Integration is disabled by default.



To enable activation of the SD-AVC cloud integration, the license token must be valid and active (not expired), and Cisco Telemetry Broker must be license-compliant, meaning it does not exceed the licensed bandwidth and is not marked "Out of Compliance".

SD-AVC integration cannot be enabled on Cisco Telemetry Broker deployment if any of the following conditions apply:



- The Cisco Telemetry Broker deployment does not have internet access.
- Licensing is managed locally via the on-premises Cisco Smart Software Manager (CSSM).
- The Smart Licensing Transport Setting is configured to use the **Transport Gateway** for outbound communication.
- The Cisco Telemetry Broker deployment is out of compliance with its smart licensing.

In these scenarios, real-time dynamic updates are unavailable, so the Cisco Telemetry Broker deployment relies on built-in application definitions. The NBAR2-based Deep Packet Inspection engine and application signatures are updated through periodic software releases to Cisco Telemetry Broker.



SD-AVC is CATO-certified and holds SOC 2 and ISO 27001 approvals. No personally identifiable information (PII) is included in the telemetry data sent to the SD-AVC backend. For more information about data sharing practices refer to the *Telemetry Matrix* section in the [Cisco SD-AVC User Guide](#).

Enable SD-AVC Integration

1. Click the  (**Settings**) icon.
The Application Settings page opens.
2. Click the **Integrations** tab.
3. Enable the **Enable SD-AVC Integration** toggle (.



When enabling SD-AVC integration, if you see the error message **License key is not available**, re-register the system using a valid smart licensing token. For more information about Re-registering, refer to the *Enable Your Telemetry Broker License* chapter in the Cisco Telemetry Broker [Virtual Appliance Deployment and Configuration Guide](#). After re-registration, you can proceed to enable SD-AVC integration.



When enabling SD-AVC after upgrading to v2.3.3, ensure your Manager is registered with a valid, non-expired smart licensing token; if the original token has expired, generate a new token via software.cisco.com, deregister the Manager, and reregister it using the new token before enabling SD-AVC.



If you see the "401 Unauthorized" error when enabling SD-AVC Integration, check the smart licensing information on the Smart Licensing page on the Manager and on software.cisco.com to make sure that the license is registered, authorized and in compliance.

User Management



External authentication is not currently supported in Cisco Telemetry Broker.

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 the user's **Email**.
5. 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.
6. 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. In the **Password** field, enter the logged-in user's password.
3. In the **Confirm Password** field, enter a new password in the **Password** field, then enter it again.
4. 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.
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"**.

Notifications

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**. If you have already configured the Syslog server, the Edit option is displayed. +
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**. If you have already configured the SMTP server, the Edit option is displayed.
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

On this page you can view information such as your name, username, email, and account status. You cannot view your password (as it is hidden), but you can change it.

How to Find This Page

In the upper right corner, click the  **Profile** button > **Profile Settings**.

The Profile Settings page opens.

Edit Account Details


To change your name or email address, complete the following steps:

1. In the Account Details section, click the  **Edit Account** button.

The Edit Account Details dialog opens.

2. Complete your edits.
3. Click **Save**.

Change Your Password

1. In the Password section, click the  **Change Password** button.

The Change Password dialog opens.

2. Complete all fields.
3. Click **Change Password**.


Change the Cisco Telemetry Broker User Interface Theme

From Cisco Telemetry Broker v2.3 release, you can now customize your viewing experience by selecting a light or dark theme for the user interface.

The theme options are:

- **Light:** Standard bright theme.
- **Dark:** Low-light theme for comfortable viewing.
- **System:** The CTB user interface automatically matches your device's system theme (for example, if your internet browser uses dark mode, the Cisco Telemetry Broker UI will also appear in dark mode).

How to Find This Page

1. In the upper right corner, click the  **Profile** button.
2. Choose your preferred theme.

How Theme Preferences are Saved

- Your selected theme is saved in your browser's settings. Each browser or device can have its own theme setting.
- If you use a different browser or device, you can set a different theme preference.
- The theme preference is not linked to your user account. If multiple users share the same browser and device, they will also share the same theme setting.

For example,

- If your device is set to dark mode and you choose "System," the UI will display in dark mode.
- If you set your browser to light mode, the UI will switch to light mode when "System" is selected.
- You can manually override this by selecting "Light" or "Dark."

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
```

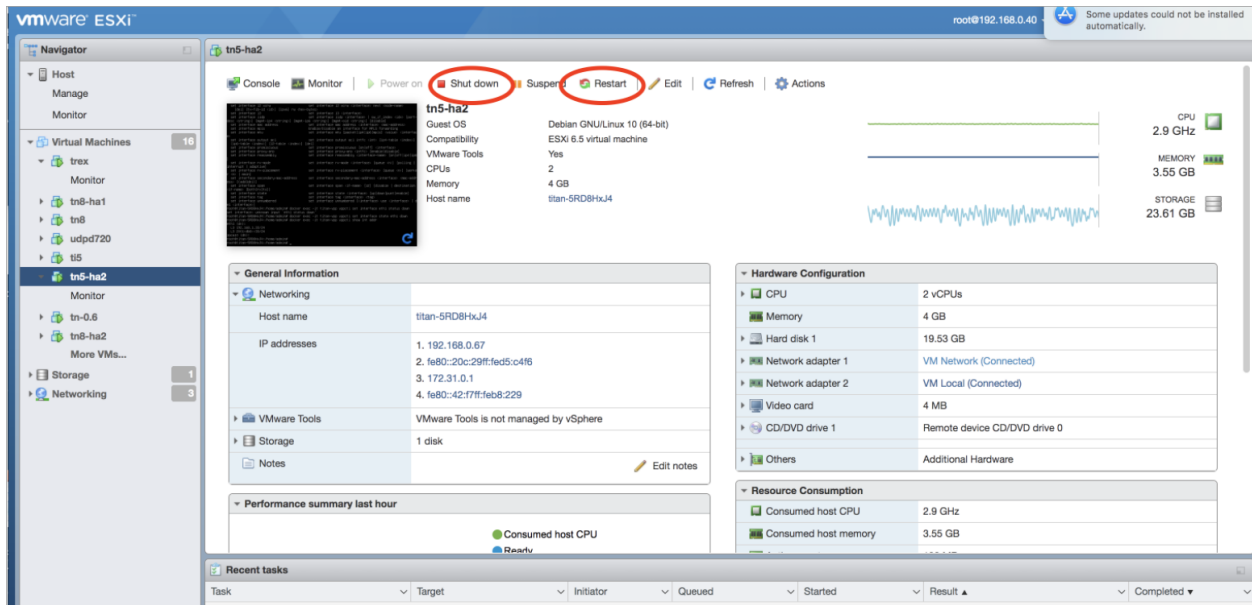
Shut Down or Reboot Cisco Telemetry Broker

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:



i External authentication is not currently supported in Cisco Telemetry Broker.

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 XDR 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	minimumIplTotalLength
26	0	maximumIplTotalLength
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
801	9	flowlogVersion_9
802	9	flowlogAccountID_9
803	9	flowlogInterfaceID_9
804	9	flowlogAction_9
805	9	flowlogLogStatus_9

ElementID	PEN	Name
806	9	flowlogVpcID_9
807	9	flowlogSubnetID_9
808	9	flowlogInstanceID_9
809	9	flowlogType_9
810	9	flowlogRegion_9
811	9	flowlogAzID_9
812	9	flowlogSublocationType_9
813	9	flowlogSublocationID_9
814	9	flowlogSystemID_9
815	9	flowlogInterfaceMac_9
816	9	flowlogRule_9
817	9	flowlogDirection_9
818	9	flowlogState_9
819	9	flowlogPktSrcAwsService_9
820	9	flowlogPktDstAwsService_9
821	9	flowlogTrafficPath_9
822	9	flowlogEncryption_9
1232	9	SGTSourceld_9
1233	9	SGTDestinationId_9
9292	9	AVCRespsCountDelta_9

ElementID	PEN	Name
9303	9	AVCSumRespTime_9
9306	9	AVCSumServerRespTime_9
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

ElementID	PEN	Name
12345	9	NVMDestinationHostname_9
12346	9	NVML4ByteCountIn_9
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

ElementID	PEN	Name
12369	9	NVMProcessArgs_9
12370	9	NVMParentProcessArgs_9
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

ElementID	PEN	Name
29807	8712	FlowSensorSourceEmailOutTrys_8712
29808	8712	FlowSensorDestinationEmailIn_8712
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

ElementID	PEN	Name
29830	8712	FlowSensorFragPktTooLong_8712
29831	8712	FlowSensorFragDifferentSizes_8712
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 Error	Config failed validation.
Destination Unreachable	This destination has sent a "destination unreachable" ICMP message.
SAS URL Close to Expiration	The input's SAS URL is about to expire. Please provide a new SAS URL.
SAS URL Expired	The input's SAS URL has expired. Please provide a new SAS URL.
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 output 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 outputs.

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

Appendix D: Differences in Types of Inputs and Outputs

Input Types

Input Type; HA- Compatible?	Max per Node or Cluster	Ingest Method	Exporter IP seen by Output	Input Details on CTB User Interface
<p>UDP;</p> <p>Yes, can be assigned to the node or cluster</p>	N/A	<p>Exporters send UDP packets to the telemetry interface.</p> <p>If input is assigned to a cluster, then exporters send UDP packets to the virtual IP address.</p>	Original exporter IP address.	<ul style="list-style-type: none"> • Exporter IP address is the original Exporter IP address • Received rate is the raw data rate
<p>VPC Flow logs;</p> <p>No, can only be assigned to the node</p>	N/A	<p>CTB fetches compressed Flow log files via the management interface using TCP.</p> <p>Flow logs are transformed to IPFIX packets and sent to applicable outputs</p>	Exporter IP address the user configured on the user interface.	<ul style="list-style-type: none"> • Exporter IP address is the one configured on the user interface by the user • Received rate is the data rate after it has been transformed

Input Type; HA- Compatible?	Max per Node or Cluster	Ingest Method	Exporter IP seen by Output	Input Details on CTB User Interface
<p>Azure Flow logs;</p> <p>No, can only be assigned to the node</p>	N/A	<p>CTB fetches Flow log data blocks via the management interface using TCP.</p> <p>Flow logs are transformed to IPFIX packets and sent to applicable outputs.</p>	<p>Exporter IP address the user configured on the user interface.</p>	<ul style="list-style-type: none"> • Exporter IP address is the one configured on the user interface by the user • Received rate is the data rate after it has been transformed
<p>Flow Generator;</p> <p>No, can only be assigned to the node</p>	1	<p>CTB sniffs traffic on the monitor interface.</p> <p>IPFIX packets are generated based on the statistics of monitored flows and sent to applicable outputs.</p>	<p>Broker node's telemetry IP address.</p>	<ul style="list-style-type: none"> • Exporter IP address is 169.254.255.100 or fd00:feed:beef::100 • Received rate is the data rate of generated IPFIX packets
<p>Proxy logs;</p> <p>Yes, can be assigned to the node or</p>	5	<p>Exporters send Proxy logs to the telemetry interface using TCP or</p>	<p>Broker node's telemetry IP address. If input is</p>	<ul style="list-style-type: none"> • Exporter IP addresses are 169.254.254.3 and fd00:feed:beef::1:3 • Received rate is the

Input Type; HA- Compatible?	Max per Node or Cluster	Ingest Method	Exporter IP seen by Output	Input Details on CTB User Interface
cluster		<p>UDP.</p> <p>If input is assigned to a cluster, then exporters send UDP packets to the virtual IP address.</p>	<p>assigned to a cluster, then it will be the telemetry IP address of the active node. When the active node is switched, the output sees a different exporter IP address.</p>	<p>data rate of IPFIX packets after they have been transformed</p>

Output Types


Output Type	Max per Node or Cluster	Data Format Specified by CTB	Output Interface	Output Details on CTB User Interface
UDP	N/A	UDP packets	Sent via the telemetry interface	<ul style="list-style-type: none"> • Sent Rate in the Metrics chart is the UDP data sent rate • You can filter the Metrics chart per exporter, input,

Output Type	Max per Node or Cluster	Data Format Specified by CTB	Output Interface	Output Details on CTB User Interface
				telemetry type, or broker node
Cisco XDR	1	Compressed files containing JSON lines	Sent via the management interface using TCP	<ul style="list-style-type: none">• Sent Rate in the Metrics chart is the compressed data sent rate• You can filter the Metrics chart per broker node only

Appendix E: AWS Configuration

You can configure your AWS deployment to export VPC Flow Logs to Cisco Telemetry Broker, then configure Cisco Telemetry Broker to transform the VPC Flow Logs to IPFIX for ingestion by outputs.

When configuring AWS Flow logs on CTB, selecting an input IP address reserves both the chosen IP and the next consecutive IP address for that flow log.

-  Consequently, the next consecutive IP address cannot be utilized for anything else on your CTB deployment. If you try to use the next consecutive IP address elsewhere on CTB, the system will display an error message.

Complete the following steps to configure your AWS portal.

Enable Flow Logging

To enable flow logging for one or more VPCs, then send the flow logs to an S3 bucket, complete the following steps:

1. From the AWS VPC main menu, choose **Your VPCs**.
2. Right-click a VPC, then choose **Create Flow Log**.
3. From the Filter drop-down, choose **All** to log accepted and rejected telemetry, or **Accept** to log only accepted telemetry.
4. Choose **Send to an S3 bucket destination**.
5. Enter an **S3 bucket ARN** in which you want to store flow log telemetry.
6. Click **Create**.

Create an IAM User

To create an IAM user that has access to the S3 bucket and record the access key ID and Secret access key, complete the following steps:

1. From the AWS IAM main menu, choose **Users > Add user**.
2. Enter a **User Name**.
3. Choose **Programmatic access**.
4. Click **Next: Permissions**.
5. Click **Next: Tags**.
6. Click **Next: Review**.
7. Click **Create User**.
8. For both the access key ID and the secret access key, click **Show**.

9. Record your Access key ID and Secret access key or click **Download** and save the keys in a secure location. You will need these keys when you create the VPC Flow Logs input in Cisco Telemetry Broker.

Create the S3 Bucket Policy

1. From the AWS IAM main menu, choose **Policies**.
2. Click **Create policy**.
3. Select the JSON tab.
4. Paste the policy you copied from Cisco Telemetry Broker into the JSON editor.
5. Click **Review policy**.
6. In the **Name** field, enter a unique name to identify the policy (for example, **ctb_policy**).
7. Enter a description, such as **Policy to allow Cisco Telemetry Broker access to VPC Flow Logs**.
8. Click **Create Policy**.

Create a User Group

To create a user group, assign the policy to an IAM group, and add your IAM user to the IAM group, complete the following steps:

1. From the AWS IAM main menu, choose **Groups > Create New Group**.
2. Enter the **group name**.
3. Click **Next Step**.
4. Select the Cisco Telemetry Broker policy that you created.
5. Click **Next Step**.
6. Click **Create Group**.
7. From the IAM console, choose **Groups > [Group Name]**.
8. Click the **Users** tab.
9. Click **Add Users to Group** and choose your **Cisco Telemetry Broker user**.
10. Click **Add Users**.

Replace S3 Bucket Code

- Replace your S3 bucket name `<s3_bucket>` with the user's actual s3 bucket name.
- Replace your S3 bucket path `< s3_path>` with the user's actual s3 bucket path.

```
"version": "2012-10-17",
"Statement": [
  {
    "Action": [
      "s3:ListBucket",
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3:::<s3_bucket>"
    ]
  },
  {
    "Action": [
      "s3:GetObject"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3:::<s3_path>/*"
    ]
  }
]
```

Appendix F: Azure Configuration

The following instructions detail how to set up a monitoring application that will collect telemetry from your Azure environment for analysis. We recommend that you follow these instructions as a user assigned the *Global Administrator AD* and *Owner* roles for all subscriptions that need monitoring.

If this isn't possible, contact your Azure AD administrator to ensure that for each subscription to be monitored, the user has access to the following Azure resources: authorization, network, storage accounts, and monitoring. For this to occur, you must assign the user the *User access administrator* and *Contributor* roles.

Prerequisites

Before configuring Azure Flow Logs, complete the following steps:

1. **Connect to Azure** Access your Azure portal and follow the instructions to sign in. For command line access, launch a bash console using the console icon located next to the search bar.
2. **Set up Network Watcher** Set up the Network Watcher service for the regions in which you have resource groups to monitor:
 - a. From the main menu, choose **Network Watcher > Overview**.
 - b. Click the **⋮ (Ellipsis)** icon and choose **Enable Network Watcher**, either at the subscription level or on target regions.
3. **Create Storage Accounts** To store Azure Flow Logs, you'll need storage accounts in the same locations (e.g. East US) as your target resource groups. If you don't already have storage accounts in the target locations, you'll need to create some with Blob storage capabilities (StorageV2 or BlobStorage).

Enable Azure Flow Logs

For the Flow Logs you want to monitor, you'll need to enable Flow Logging by completing the following steps:

1. From the main menu, choose **Network Watcher > Logs > Flow Logs**. The list of already enabled Flow logs appears.
2. To create a new flow log, click **+Create** button.
3. Complete the form, entering the following settings:

- **Subscription:** Select your subscription.
- **Flow log type:** Select **Virtual Network**. You can no longer create new Network Security Group flow logs starting June 30, 2025. Your existing Network Security Groups (NSGs) can continue to work till September 30, 2027, but we recommend you switch to Virtual Network (VNet) as soon as possible.



Note that Microsoft recommends disabling Network Security Group Flow Logs before enabling Virtual Network Flow Logs on the same underlying workloads to avoid duplicate traffic recording and additional costs.

- **Select Target Resource:** Click **Virtual Network**, **Subnet**, or **Network Interface** based on your desired monitor level. The **Select virtual network** page or **Select subnet** page or **Select network interface** page appears.
 - Select one or more resources that you want to enable and click **Confirm Selection**.
 - **Select Storage account:** Select the **Location**, **Subscription**, and **Storage accounts**.
 - **Retention (days):** Enter the number of days you want to retain data. If you want to retain data forever and do not want to apply a retention policy, set **Retention (days)** to 0.
 - Click **Next: Analytics >** and clear **Enable Traffic Analytics**.
 - Click **Review + Create**.
 - Click **Create**.
4. In **Network Watcher > Logs > Flow Logs** page, you will see new enabled flow logs, with **Flow log type** as **Virtual Network**.



Repeat steps 1 to 4 for each Network security group(s) that you want to enable.

5. In the Azure portal, from the main menu, choose **Storage Accounts > Select Your Account > Data Storage > Containers**. Verify that you see the *insights-logs-flowlogflowevent* entry in the Containers list. It may take a few minutes for it to appear.



It might take about 10 minutes for the flow logs to be published. You can navigate through the Tree View to see if the newly enabled Flow Logs have published their flow log files.

Obtain Blob Service SAS URL

To generate the Blob Service SAS URL that Cisco Telemetry Broker requires, complete the following steps:

1. In the Azure portal, from the main menu, choose **Storage Accounts > Select Your Account > Shared Access Signature**. The form that opens should contain the following entries:
 - **Allowed Services:** Blob
 - **Allowed Resource Types:** Service, Container, Object
 - **Allowed Permissions:** Read, List
 - **Start and Expiry Times:** Set to an interval that you will allow Cisco Telemetry Broker to access
2. Choose **Generate SAS > the connection string**.
3. Copy the Blob Service SAS URL.



Provide the Blob Service SAS URL when adding the Azure Flow Log to Cisco Telemetry Broker.

Register Azure Flow Log in Cisco Telemetry Broker

To configure Cisco Telemetry Broker to process the Azure Flow Log telemetry and transform it into IPFIX, complete the following steps:

1. Return to Cisco Telemetry Broker.
2. From the Cisco Telemetry Broker Explorer, click the broker node that you want to add Azure Flow Log input, and click the **Inputs** tab.
3. Click the **+ Add Input** button (located above the Inputs table in the upper right corner).

*The **Add Input** dialog opens.*
4. Select **Azure Flow Log** and click **Next**.
5. In the **Input Name** field, enter the input name.
6. In the **Blob Service SAS URL** field, enter the Blob Service SAS URL copied from Azure portal.
7. In the **Input IP Address** field, enter the input IP address to assign to this Flow Log. Cisco Telemetry Broker uses this IP address as the input address when sending

IPFIX generated from the Azure Flow Log. It should be an internal IP address and should not conflict with other IP addresses on your network.

Cisco Telemetry Broker places the following restrictions on the Input IP value to ensure proper brokering of packets. If any of the following conditions are not met, Cisco Telemetry Broker displays an error message:

- Input IP must **not** overlap with the subnet of the Assigned Node's Telemetry interface.
- Input IP must **not** conflict with any existing input IPs in the system.
- Input IP must **not** conflict with any output IPs in the system.



When configuring Azure Flow logs on CTB, selecting an input IP address reserves both the chosen IP and the next consecutive IP address for that flow log. Consequently, the next consecutive IP address cannot be utilized for anything else on your CTB deployment. If you try to use the next consecutive IP address elsewhere on CTB, the system will display an error message.

8. From the **Azure Flow Log Type** drop-down list, select **Virtual Network**.



If you have NSG Flow Logs enabled on your Azure portal, you still can add **Azure Flow Log** input with **Network Security Group** type. It will continue to work till NSG retirement date of September 30, 2027. But you need to make sure the type selected here matches the type you selected in your Azure portal. If the storage account that you created Blob SAS URL has both Virtual network container and NSG container, broker node only fetches the Flow Logs of the type configured for the input.

9. Click **Add Input**.
10. If you have multiple Azure Flow Logs to configure, complete the following steps, in order, for each Azure Flow Log you configure:
 - a. Repeat every step in each previous section in this [Azure Configuration](#) topic.
 - b. Repeat Step 1 through Step 8 in this section.

Appendix G: Proxy Log Input Configuration Guide

A web proxy server can send log messages to a proxy log input in Cisco Telemetry Broker. These log messages are parsed based on configured regex patterns and then transformed to IPFIX packets.

Proxy log inputs always show exporters as 169.254.254.3 and fd00:feed:beef::1:3 in the Cisco Telemetry Broker Manager web interface, but outputs see IPFIX packet source IP address as the associated broker node's telemetry IP address. The web proxy's IP address appears in the IE exporterIPv4Address or exporterIPv6Address to outputs.

You can connect a proxy log input to one or more outputs configured in Cisco Telemetry Broker. Note the following parameters:

- If a proxy log message is received as an IPv4 packet, it will be forwarded to only IPv4 UDP outputs.
- If a proxy log message is received as an IPv6 packet, it will be forwarded to only IPv6 UDP outputs.



Although Cisco Telemetry Broker allows connecting Proxy Log Input to Cisco XDR outputs, it is not recommended to do so because Cisco XDR does not currently support analytics based on proxy log messages.

Web Proxy Server-side Requirements

You need to configure your server-side web proxy so that it includes the following information in log messages:

- sourceIPAddress
- sourceTransportPort
- destinationIPAddress
- clientOctetDeltaCount (HTTP request direction)
- serverOctetDeltaCount (HTTP response direction)
- method
- url
- responseCode

- duration
- userName

The following are optional fields:

- ts (timestamp)
- contentType
- clientDeltaPacketCount
- serverPacketDeltaCount
- protocol
- scheme
- destinationTransportPort

Cisco Telemetry Broker does not use any other user-defined field in log messages to form IPFIX packets.

IPFIX Templates

We use eight IPFIX templates. Each template has three IP addresses. These can be either all IPv4, all IPv6, or a combination of both. There exists a total of eight different combinations. Refer to the following table when constructing regex patterns and to understand IPFIX flow records.

Variable Name	IE (PEN)	Notes
sourceIPv4Address OR sourceIPv4Address	8 OR 27	Parsed from proxy log message.
destinationIPv4Address OR destinationIPv6Address	12 OR 28	
sourceTransportPort	7	Parsed from proxy log message.
destinationTransportPort	11	Parsed from proxy log message. If this is missing, then 443 or 80 is used (based on

		protocol/scheme/method/url).
octetDeltaCount	1	Parsed from proxy log message.
packetDeltaCount	2	Parsed from proxy log message. If this is missing, then it is estimated based on octetDeltaCount and average packet size.
ingressinterface	10	Use 1.
egressinterface	14	Use 1.
protocolIdentifier	4	Use 6.
tcpControlBits	6	Use 0x13 (c2s) OR 0x18 (s2c).
applicationId	95	4 bytes NBAR ID for proxy server (218104888).
flowSensorApplicationDetails	29832 (PEN 8712)	c2s: method + url + proxy_vendor_info + protocol that proxy uses to send message to Cisco Telemetry Broker. s2c: response_code + proxy_vendor_info + protocol that proxy uses to send message to Cisco Telemetry Broker.
flowStartMilliseconds	152	Use (flowEndMilliseconds-duration).
flowEndMilliseconds	153	Use current time.
ipClassOfService	5	Use 5.
exporterIPv4Address OR exporterIPv6Address	130 OR 131	Source IP address of the log message packet that Cisco Telemetry Broker receives.

userName	371	Parsed from proxy log message. If these are missing, then set this to an empty string.
----------	-----	--

Configuration Parameters

When you choose a proxy log input, you need to configure the following parameters:

- Input name.
- Port: The port to listen on needs to be unique for each broker node (or cluster of nodes).
- Vendor: Proxy server name and version, up to 64 characters.
- Protocol: TCP or UDP.
- Mapping: Use regex patterns to parse log messages. We provide example mappings for some proxy servers, but you will need to create your own mappings based on the log format your server sends out. See the next section, [Configure Your Own Regex Patterns/Mappings](#).
- Average Packet Size: If the log message does not include the **clientDeltaPacketCount** field or **serverDeltaPacketCount** field, Cisco Telemetry Broker estimates the **clientDeltaPacketCount** field or **serverDeltaPacketCount** field using the **clientOctetDeltaCount** field or the **serverOctetDeltaCount** and **Average Packet Size** fields.

Configure Your Own regex Patterns/Mappings

The patterns and mappings in the Dropdown options list are only examples and probably won't fit your actual log format. You may need to create your own regex patterns.

To do this, follow these steps:

1. Go to https://<ctb_manager>/backend/admin.
2. After you log in, find the Dropdown options list.



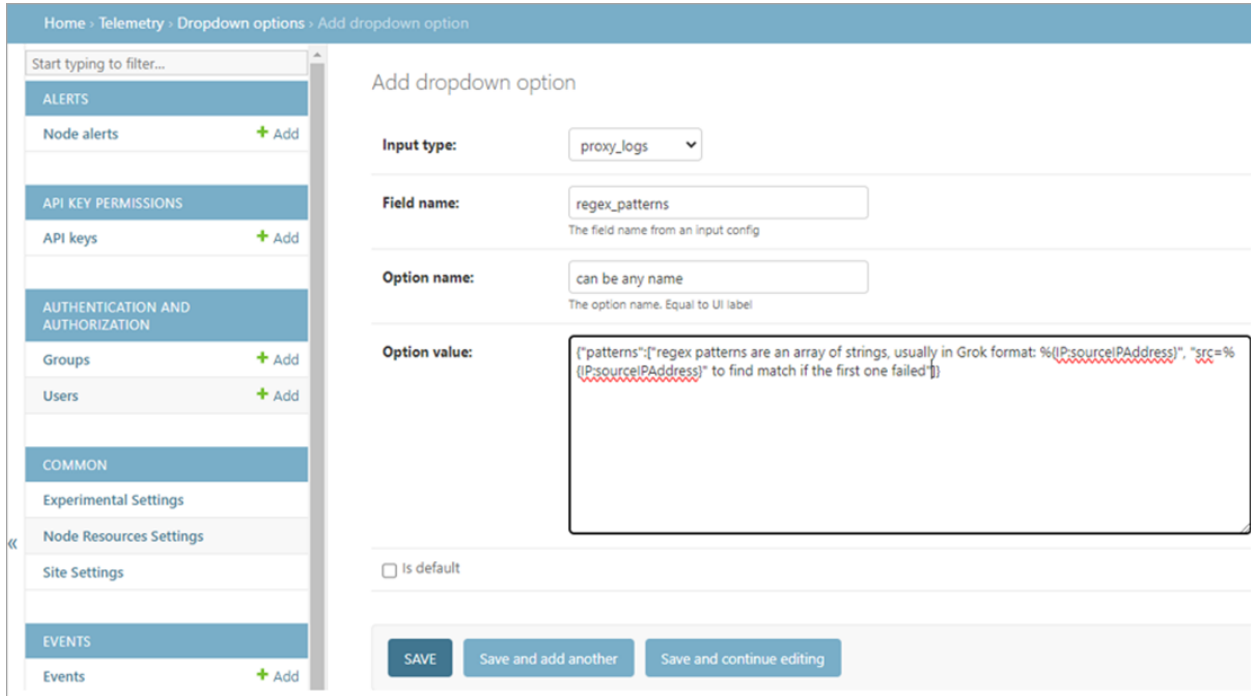
3. To add a dropdown option, click **Add**.

*The following appears if you click **Add**.*



4. Click **ADD DROPDOWN OPTION +**.

The following page opens on which you can add the regex patterns/mappings:



5. When finished, click **SAVE**. The regex patterns/mappings are now available in the Proxy Logs Input dialog.

Regex Patterns and Field Transform Algorithms

Pattern/Field Transform Algorithm	Example
<p>Grok regex format: <code>{PATTERN_NAME:variable_name[:type]}</code></p>	<p>dstport=% {NONNEGINT:destinationTransportPort:int} would match "dstport=8088" and map resulting integer to destinationTransportPort=8088</p>

Pattern/Field Transform Algorithm	Example
<p>If no Grok pattern is readily available, you can define custom patterns:</p> <p><PATTERN NAME> <regex definition><newline></p>	<p>ANYTEXT[^\]]*\nTZ (?:[PMCEG][SDM]T UTC)</p>
<p>You can use the two customer regex definitions (ANYTEXT and TZ) in the following regex pattern:</p>	<p>devicetime=\\[%{DATE:date}%{TIME:time}%{TZ:timezone}:\\ \\ url=%{ANYTEXT:url}</p> <p>would match the following log</p> <p>devicetime=[26/08/2014:14:52:08 GMT] url=http://pixel.digitserve.com/pixel;r=1</p> <p>Results:</p> <p>date="26/08/2014"</p> <p>time="14:52:08"</p> <p>timezone="GMT"</p> <p>url="http://pixel.digitserve.com/pixel;r=1"</p> <p>You can apply transform algorithms to the parsed results to infer certain IPFIX required fields (which are otherwise missing) to form IPFIX packets.</p> <p>See below for the four transform algorithms that are available for you to use:</p>
<p>Four Transform Algorithms</p> <p>{“key”: {“0”: value}} -- Assign a constant value to a field of key, “0” is this transform id</p> <p>{“key”: {“1”: “key1”}} -- Assign value of a field of key1 to field of key, “1” is this transform id</p> <p>{“key”: {“2”: {“key1”: {“cond1”: value1, “cond2”: value2}}}} – Assign value based on field value of key1 to target field of key, “2” is this transform id</p>	

Pattern/Field Transform Algorithm	Example
<pre>{“key”: {“3”: {op: {“key1”: value1}}}} -- Perform arithmetic operations to field of key1 to another field of key, “3” is this transform id, op: 1: multiply 2: divide 3: add 4: subtract</pre>	

Performance

The table below outlines the capabilities achievable in an idealized test environment. This setup assumes a Cisco Telemetry Broker deployment dedicated to ingesting and transforming proxy logs, with the specified resources allocated to the virtual broker node.

- 8 reserved CPUs, 8 cores per socket
- 12 GB RAM, all reserved
- VMXNET3 telemetry interface
- 1 proxy log input sending to 1 UDP output
- 0 XDR outputs
- 0 Flow Generator Inputs

Mapping	UDP (pps)	TCP (pps)
Bluecoat Example	5000	28000
Cisco Example	7500	29000
Forcepoint Example	4250	25000
JSON Example	6000	29000
McAfee Example	7500	24500
Squid Example	7500	21500
Zscaler Example	7500	23000

UDP Pass/Fail threshold: (missing packets/sent packets) < 0.00001

Recommendations to achieve the best performance:

- Use the TCP protocol as it performs 3-5 times better than UDP.
- Alter your proxy server to send logs that match one of our example patterns. Adding a custom regex pattern will bypass Cisco Telemetry Broker's fast parsing and will be 2-4 times slower for TCP (and 50% slower for UDP).

Appendix H: Flow Log Format Fields to IPFIX IE Mapping

Flow Logs Format Field	IPFIX Information Element Name (ID)	IPFIX Enterprise ID	IPFIX IE Type	Notes	Applicable To
version	flowlogVersion (801)	Cisco Systems (9)	Unsigned8		AWS, Azure
account-id	flowlogAccount ID (802)	Cisco Systems (9)	string	Up to 36 characters	AWS
interface-id	flowlog Interface ID (803)	Cisco Systems (9)	string	Up to 36 characters	AWS
srcaddr	sourceIPv4 Address (8)	N/A	ip4_address_t	4 bytes, ipv4 templates only	AWS, Azure
	OR the following:				
	sourceIPv6 Address (27)	N/A	ip6_address_t	16 bytes, ipv6 templates only	AWS, Azure
dstaddr	sourceIPv4 Address (12)	N/A	ip4_address_t	4 bytes, ipv4 templates only	AWS, Azure
	OR the following:				
	sourceIPv6	N/A	ip6_	16 bytes,	AWS,

Flow Logs Format Field	IPFIX Information Element Name (ID)	IPFIX Enterprise ID	IPFIX IE Type	Notes	Applicable To
	Address (28)		address_t	ipv6 templates only	Azure
srcport	source TransportPort (11)	N/A	unsigned16		AWS, Azure
dstport	destination TransportPort (11)	N/A	unsigned16		AWS, Azure
protocol	protocol Identifier(4)	N/A	unsigned8		AWS, Azure
packets	packetDelta Count (2)	N/A	unsigned64		AWS, Azure
bytes	octetDelta Count (1)	N/A	unsigned64		AWS, Azure
start	flowStart Seconds (150)	N/A	unsigned32		AWS, Azure
end	flowEnd Seconds (151)	N/A	unsigned32		AWS, Azure
action	flowlog Action (804)	Cisco Systems (9)	string	up to 36 characters	AWS, Azure
log-status	flowlogLog Status (805)	Cisco Systems (9)	string	up to 36 characters	AWS
vpc-id	flowlog	Cisco	string	up to 36	AWS

Flow Logs Format Field	IPFIX Information Element Name (ID)	IPFIX Enterprise ID	IPFIX IE Type	Notes	Applicable To
	VPCID (806)	Systems (9)		characters	
subnet-id	flowlog SubnetID (807)	Cisco Systems (9)	string	up to 36 characters	AWS
instance-id	flowlog InstanceID (808)	Cisco Systems (9)	string	up to 36 characters	AWS
tcp-flags	tcpControl Bits (6)	N/A	unsigned16		AWS
type	flowlogType (809)	Cisco Systems (9)	string	up to 36 characters	AWS
pkt-srcaddr	postNAT SourceIPv4 Address (225)	N/A	ip4_address_t	4 bytes, ipv4 templates only	AWS
	Or the following:				
	postNAT DestinationIPv6 Address (281)	N/A	ip6_address_t	16 bytes, ipv6 templates only	AWS
pkt-dstaddr	postNAT DestinationIPv4 Address (226)	N/A	ip4_address_t	16 bytes, ipv6 templates only	AWS
	Or the following:				

Flow Logs Format Field	IPFIX Information Element Name (ID)	IPFIX Enterprise ID	IPFIX IE Type	Notes	Applicable To
	postNAT DestinationIPv6 Address (282)	N/A	Ip6_address_t	16 bytes, ipv6 templates only	AWS
region	flowlog Region (810)	Cisco Systems (9)	string	up to 36 characters	AWS
az-id	flowlogAzID (811)	Cisco Systems (9)	string	up to 36 characters	AWS
sublocation-type	flowlog Sublocation Type (812)	Cisco Systems (9)	string	up to 36 characters	AWS
sublocation-id	flowlog Sublocation ID (813)	Cisco Systems (9)	string	up to 36 characters	AWS
system-id	flowlog SystemID (814)	Cisco Systems (9)	string	up to 36 characters	Azure
intf-mac	flowlog InterfaceMAC (815)	Cisco Systems (9)	macAddresses	6 bytes	Azure
rule	flowlogRule (816)	Cisco Systems (9)	string	up to 36 characters	Azure
flow-direction	flowlog Direction (817)	Cisco Systems (9)	string	up to 36 characters	AWS, Azure

Flow Logs Format Field	IPFIX Information Element Name (ID)	IPFIX Enterprise ID	IPFIX IE Type	Notes	Applicable To
state	flowlogState (818)	Cisco Systems (9)	string	up to 36 characters	Azure
pkt-src aws-service	flowlogPktSrc AwsService (819)	Cisco Systems (9)	string	up to 36 characters	AWS
pkt-dst aws-service	flowlogPktDst AwsService (820)	Cisco Systems (9)	string	up to 36 characters	AWS
traffic-path	flowlogTraffic Path (821)	Cisco Systems (9)	string	up to 36 characters	AWS
flow encryption	flowlogEncryption (822)	Cisco Systems (9)	string	up to 36 characters	Azure

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
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Change History

Document Version	Published Date	Description
1_0	September 29, 2025	Initial Version.
1_1	October 13, 2025	Minor Updates.

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)

