



Cisco Telemetry Broker

Release Notes 2.3.3




Table of Contents

Introduction	3
What's New In This Release	4
What's New in v2.3.3	4
Support for Dark Theme Selection in Cisco Telemetry Broker User Interface	4
Changes In Output Configuration	4
Per-Node HTTPS Proxy Configuration	4
Application Classification and SD-AVC Integration	4
Support for Azure VNet Flow Logs	5
Improved Proxy Log Input Performance	5
Before You Update to v2.3.3	6
Azure Flow Log Inputs	6
SD-AVC Integration	6
Output Configuration	7
Deprecation of CLI-Based Configuration Migration	7
HTTPS Proxy Configuration	8
Change in Landing Page URL	8
IPv6 Support for Smart Licensing	8
Virtual Machine Requirements	8
Upgrade Your Cisco Telemetry Broker Deployment	10
Download the Update File	10
Upload the Update File	11
What's Been Fixed	12
Fixed Issues in v2.3.3	12
Known Issues	13
Known Issues in v2.3.3	13
Change History	16
Release Support Information	17

Introduction

This document provides information about the new features and improvements, bug fixes, and known issues for the v2.3.3 release of Cisco Telemetry Broker.

 To review release notes for previous releases, go [here](#).

For additional information about Cisco Telemetry Broker, go to cisco.com.

What's New In This Release

What's New in v2.3.3

These are the new features, improvements, and changes made for the Cisco Telemetry Broker v2.3.3 release.

Support for Dark Theme Selection in Cisco Telemetry Broker User Interface

This release of Cisco Telemetry Broker introduces the dark mode, giving you more control over the viewing experience. Alongside the default light mode, you can now choose between light, dark, or system themes. The system theme option automatically adapts the UI to match your device's current appearance settings, ensuring a seamless and personalized interface whether you're working in bright or low-light environments.

Changes In Output Configuration

This release introduces significant changes to how data flows are managed within Cisco Telemetry Broker. The terminology has been updated for improved clarity: *destinations* are now referred to as *outputs*. Outputs are now local to broker nodes or clusters, providing more precise control over where each broker node sends its data. The user interface has been enhanced to reflect these changes, offering a clearer and more intuitive hierarchical view of all configured inputs and outputs.

Additionally, the system now supports backup and restore operations between systems running the same version, improving reliability and disaster recovery options.

Per-Node HTTPS Proxy Configuration

Cisco Telemetry Broker now supports per-node proxy configuration, enabling you to configure individual proxy settings for each broker and manager node. This enhancement replaces the previous system-wide (global) proxy setup, providing greater flexibility for complex network environments.

Application Classification and SD-AVC Integration

The Flow Generator input now offers 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.


Support for Azure VNet Flow Logs

Cisco Telemetry Broker v2.3.3 significantly enhances its integration with Microsoft Azure by introducing support for Azure VNET (Virtual Network) Flow Logs. When configuring new Azure Flow Log inputs, you will now find a new dropdown menu allowing you to explicitly select the "Azure Flow Log Type" as either Network Security Group or Virtual Network. This provides flexibility to integrate with both legacy and modern Azure Flow Log deployments.

Improved Proxy Log Input Performance

When using one of the provided mappings, packets delivered via TCP from a proxy server can be processed 2-4 times faster than Cisco Telemetry Broker v2.2.1.

Before You Update to v2.3.3


-  You can only upgrade to Cisco Telemetry Broker v2.3.3 if your deployment is running v2.2.1. If you are running an older version, you must first upgrade to v2.2.1 before you can install v2.3.3.

Before you begin the update process to v2.3.3, it is important to note the following.

Azure Flow Log Inputs

With the release of v2.3.3, we've introduced support for Azure VNET (Virtual Network) Flow Logs, aligning with Microsoft's evolving standards. Please be aware of the following behavior during and after your upgrade:

- Default Behavior for Existing Inputs: Upon upgrading your Cisco Telemetry Broker deployment to v2.3.3, all your pre-existing Azure Flow Log inputs will automatically be migrated. For these inputs, the Azure Flow Log Type setting will default to NSG. This ensures that your current data ingestion from Azure NSG Flow Logs continues uninterrupted immediately after the upgrade.
- If you have already migrated your Azure environment to use VNET Flow Logs, or if you plan to do so, you must perform an additional step after upgrading CTB to v2.3.3:
 - First, ensure your Azure environment is configured to send VNET Flow Logs.

 Note that you might need to generate new SAS URL if VNET Flow Logs use different storage.

- Then, within Cisco Telemetry Broker, you can either edit relevant NSG Flow Log input configuration or delete the relevant NSG Flow Log input and create a new VNET Flow Log input.
- If you choose to edit, within Cisco Telemetry Broker, navigate to each relevant Azure Flow Log input, edit its configuration, and manually change the "Azure Flow Log Type" from **Network Security Group** to **Virtual Network**, and change SAS URL if needed.

SD-AVC Integration

If Smart Licensing was already enabled and registered, both application classification and SD-AVC integration will be available after the upgrade. These settings are disabled by default.

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) and 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.



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.

Output Configuration

During the upgrade to v2.3.3, only outputs (formerly known as destinations) that are assigned to at least one input will be migrated. Any outputs that are not connected to an input (i.e., unassigned or global outputs) will be removed during the upgrade process.



To prevent the deletion of any destinations during the upgrade, you may temporarily assign any unassigned outputs to an existing input before proceeding with the upgrade. This will ensure that all your desired outputs are retained during the migration process.



Before upgrading to v2.3.3, it is recommended to remove all unreachable destinations. This helps prevent legacy alerts from remaining after the upgrade, particularly when destinations have been automatically removed or reassigned during migration.

If unreachable destinations are not cleared prior to the upgrade, you may encounter stale alerts post-upgrade, that can only be resolved by manually removing and recreating the affected outputs after the upgrade.

Deprecation of CLI-Based Configuration Migration

Migrating configuration to a new System via CLI is deprecated in v2.3.3. Configuration backup and restoration is now performed using the Cisco Telemetry Broker user interface.

HTTPS Proxy Configuration

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

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

The manager node proxy and each broker node proxy must be configured separately after the upgrade from v2.2.1.

Change in Landing Page URL

Starting with CTB v2.3.3, the default page URL has changed from */overview* to */dashboard*. If you have bookmarks with */overview*, you will see a 404 error page, but you can still navigate normally using other menus. It is recommended that you update your bookmarks to */dashboard* in the URL instead of */overview* to avoid this issue.

IPv6 Support for Smart Licensing

Smart Licensing supports IPv6, enabling devices to use IPv6 addresses for communication with Cisco Smart Software Manager (CSSM). IPv6 CTB instances using an IPV6 proxy address can communicate with CSSM for a successful Smart Licensing registration.

Virtual Machine Requirements

For virtual deployments, starting with v2.3.3, a broker node VM requires an x86 64-bit CPU with Advanced Vector Extensions (AVX) instruction set support. You need to configure the VM to expose the AVX instruction set.

For KVM:

To ensure that the AVX instruction set is available in a VM running on KVM via the UI (virt-manager/Virtual Machine Manager), follow these steps:

1. Open the VM in Virtual Machine Manager (`virt-manager`).
2. Launch Virtual Machine Manager on your KVM host.
3. Right-click your VM and select Shut Down (if it is running).
4. Right-click again and choose **Open** or **Details**.
5. Edit CPU Settings
6. In the left sidebar, select "Processor" or "CPUs".

7. Look for the "Configuration" or "Model" section.
8. Set CPU Model to "host-passthrough" or "Copy host CPU configuration"



It is recommended to select the **Copy host CPU configuration** or **host-passthrough** option. This will expose all CPU features (including AVX) from the host to the VM.

For VMWare:

Run the following command to verify that the AVX instruction set is available in VM:

```
$ if grep -q avx /proc/cpuinfo; then echo "AVX enabled!"; else echo "AVX disabled!"; fi
```

If the CPU AVX instruction set is not available in the VM, do the following:

- Ensure the VM compatibility setting is new enough to support AVX instructions, for example, Version 17 for ESXi 7.0
- Ensure the VM's CPU selection is new enough to support AVX instructions. Using vSphere, go to the VM's Configure tab, select VMware EVC, and change the CPU Mode to Haswell CPU or newer for Intel processors, and to Opteron CPU or newer for AMD processors.

vSphere Enhanced vMotion Compatibility (EVC) ensures live migration of workloads using vMotion between ESXi hosts within a cluster, even if they are running different CPU generations.

The screenshot shows the vSphere configuration interface for a VM named 'ctb-broker-node-sca-244'. The 'Configure' tab is selected, and the 'VMware EVC' section is highlighted in the left-hand menu. The main content area displays 'VMware EVC is Disabled' with an 'EDIT...' button to the right. The left-hand menu includes options like VM SDRS Rules, vApp Options, Alarm Definitions, Scheduled Tasks, Policies, VMware EVC (selected), and Guest User Mappings.

Change EVC Mode | ctb-broker-node-sca-244



Select EVC Mode

Disable EVC
 Enable EVC for AMD hosts
 Enable EVC for Intel® hosts

CPU Mode

Intel® "Haswell" Generation

Description

CPU Mode

Applies the baseline feature set of Intel® "Haswell" Generation processors to all hosts in the cluster.

Hosts with the following processor types will be permitted to enter the cluster:

Intel® "Haswell" Generation
 Intel® "Broadwell" Generation
 Intel® "Skylake" Generation
 Future Intel® processors

Compared to the Intel® "Ivy Bridge" Generation EVC mode, this EVC mode exposes additional CPU features including Advanced Vector Extensions 2, fused multiply-adds, Transactional Synchronization Extensions, and new bit manipulation instructions.

Note: Some "Haswell" microarchitecture processors do not provide the full "Haswell" feature set. Such processors do not support this EVC mode; they will only be admitted to the Intel® "Nehalem" Generation mode or below.

For more information, see Knowledge Base article 1003212.

CANCEL

OK

Upgrade Your Cisco Telemetry Broker Deployment

The Software Update page in your Cisco Telemetry Broker manager web interface 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 update, and updates your manager first, then the broker nodes. While your manager updates, you may not see the proper state of your Cisco Telemetry Broker deployment. While each broker nodes updates, it will not pass traffic to destinations.

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. Select 2.3.3 from the left-hand navigation pane
5. Choose the **Manager Node Software**.
6. Download the CTB Update Bundle file: **ctb-update-bundle-v2.3.3-0-g0b78a7f.prod.secured.tar**.

 You can install the v2.3.3 bundle file in Cisco Telemetry Broker v2.2.1 only.

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. 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 per appliance.

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.

What's Been Fixed

This section provides information about the bugs (defects) which are fixed in this release. For each defect, there is a corresponding Cisco Defect and Enhancement Tracking System (CDETS) number. Click the CDETS link to view details about an issue.

Fixed Issues in v2.3.3


CDETS ID	Description
CSCwp34129	Support for Azure Virtual Network Flow Logs are added in Cisco Telemetry Broker.
CSCwo07023	Log files in the proxylogs plugin folder are included in the mayday diagnostic pack.

Known Issues

This section summarizes issues (bugs) that are known to exist in Cisco Telemetry Broker. Where possible, workarounds are included.

Known Issues in v2.3.3

CDETS ID	Description and Workaround
CSCwq48897	<p>Description</p> <p>After upgrading to CTB v2.3.3 from an intermediate build, the smart licensing registration token may disappear, causing the "License key is not available" error when enabling SD-AVC; re-registering with a valid token resolves this.</p> <p>Workaround</p> <p>The issue can be resolved by re-registering the system to the Cisco Smart Software License portal with a valid smart licensing token. It can be the same token used previously; it does not have to be a new token.</p>
CSCwq48917	<p>Description</p> <p>Creating an AWS VPC Flow Log input on a CTB manager node without internet or proper proxy access causes the system to become unresponsive.</p> <p>Workaround</p> <p>Ensure the CTB manager's management interface has internet access to reach AWS, and if a proxy is needed, configure the HTTPS Proxy setting on the Manager Node Details page with the correct proxy address and port.</p>
CSCwq60358	<p>SAPY Agent initialization keeps failing after PLR registration</p> <p>Workaround</p> <div style="border: 1px solid orange; padding: 10px;"> <p>Use these commands with CAUTION and ONLY if you need to make licensing changes on an ALREADY PLR REGISTERED SYSTEM. This will:</p> <ul style="list-style-type: none"> - Remove the existing PLR registered SMART agent from the </div>

CDETS ID	Description and Workaround
	<div style="border: 1px solid orange; padding: 10px; margin-bottom: 10px;"> <p>database</p> <ul style="list-style-type: none">  - Reset the system to a clean unregistered state - Require removing the license from CSSM </div> <p>Execute Fix on Manager Node:</p> <ol style="list-style-type: none"> 1. Switch to root user <code>sudo su</code> 2. Remove licensing configuration file <code>rm /var/lib/titan/titanium/licensing/licensing.json</code> 3. Clean database entries <code>sudo docker exec -it postgres psql -U postgres</code> 4. In the PostgreSQL shell, execute: <code>delete from licensing_agentprovider;</code> <code>delete from licensing_agentstate;</code> <code>exit</code> 5. Restart services <code>systemctl restart titan-compose</code> <p>Post-Resolution Verification</p> <ul style="list-style-type: none"> • After restart, the SL (Smart Licensing) page in the UI must return to "Unregistered" state. • You need to manually remove the PLR reservation in CSSM.
No associated ID	<p>Description</p> <p>After upgrading to CTB v2.3.3, existing alerts for non-existing UDP destinations may not be deleted even if the destination has been removed automatically during the migration. Specifically, a dead destination alert can appear for a UDP Destination IPv6 assigned to a different broker node than indicated in the alert. Enabling or disabling the Output's reachability check does not clear the alert.</p> <p>Workaround</p> <p>Before upgrading to CTB v2.3.3, remove all unreachable UDP</p>

CDETS ID	Description and Workaround
	destinations to prevent persistent dead destination alerts after the upgrade.
No associated ID	<p>Description</p> <p>Syslog Server Unreachable When Using FQDN Without IPv6 Configured.</p> <p>If the syslog server is specified using a domain name (FQDN) and the management interface does not have an IPv6 address configured, the server may be unreachable.</p>

Change History

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

Release Support Information

Official General Availability (GA) date for Release 2.3.3 is October 2025.

For support timeline information regarding general software maintenance support, patches, general maintenance releases, or other information regarding Cisco Telemetry Broker Release Support lifecycle, please refer to the [Cisco Telemetry Broker Software Lifecycle Support Statement](#).

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)