# Release Notes for Cisco Catalyst 8300 Series Edge Platforms, Cisco IOS XE Bengaluru 17.5.x

**First Published:** 2021-03-22

## About Cisco Catalyst 8300 Series Edge Platforms

The Cisco Catalyst 8300 Series Edge Platforms are best-of-breed, 5G-ready, cloud edge platforms designed for accelerated services, multi-layer security, cloud-native agility, and edge intelligence to accelerate your journey to cloud.

Cisco Catalyst 8300 Series Edge Platforms with Cisco IOS XE SD-WAN Software deliver Cisco's secure, cloud-scale SD-WAN solution for the branch. The Cisco Catalyst 8300 Series Edge Platforms is built for high performance and integrated SD-WAN Services along with flexibility to deliver security and networking services together from the cloud or on premises. It provides higher WAN port density and a redundant power supply capability. The Cisco Catalyst 8300 Series Edge Platforms have a wide variety of interface options to choose from—ranging from lower and higher module density with backward compatibility to a variety of existing WAN, LAN, voice, and compute modules. Powered by Cisco IOS XE, fully programmable software architecture, and API support, these platforms can facilitate automation at scale to achieve zero-touch IT capability while migrating workloads to the cloud. The Cisco Catalyst 8300 Series Edge Platforms also come with Trustworthy Solutions 2.0 infrastructure that secures the platforms against threats and vulnerabilities with integrity verification and remediation of threats.

The Cisco Catalyst 8300 Series Edge Platforms are well suited for medium-sized and large enterprise branch offices for high WAN IPSec performance with integrated SD-WAN services.

For more information on the features and specifications of Cisco Catalyst 8300 Series Edge Platforms, refer to the Cisco Catalyst 8300 Series Edge platforms datasheet.

**Note** Sections in this documentation apply to all models of Cisco Catalyst 8300 Series Edge Platforms unless a reference to a specific model is made explicitly.

**Note** Cisco IOS XE Bengaluru 17.5.1a is the first release for Cisco Catalyst 8300 Series Edge Platforms.

## Hardware and Software Features-New and Enhanced

### New and Changed Hardware Features

There are no new hardware features in this release.

For information on the hardware features supported on the NIM-PVDM, refer to the Cisco Packet Voice Digital Signal Processor Modules for Cisco Unified Communications Solutions datasheet.

# New and Changed Software Features

This section enlists the new and enhanced or modified features that are supported on the Cisco Catalyst 8300 Series Edge Platforms:

## Feature Navigator

You can use Cisco Feature Navigator (CFN) to find information about the software features, platform, and software image support on Cisco Catalyst 8300 Series Edge Platforms. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.

**Note** To access CFN, you do not require an account on cisco.com.

# Software Features

***Table 1: New Software Features in Release Cisco IOS XE Bengaluru 17.5.1***

| Feature | Description |
|---|---|
| Capability to limit IPv6 Mroutes Per VRF | This feature lets you configure a limit to the number of mroutes on an interface. By limiting the mroutes, you can avoid the risk of flooding the network with mroutes therefore protecting the router from resource overload and also preventing DoS attacks. |
| Cisco IS-IS Local Unequal Cost Multipath | The Segment Routing—IS-IS UCMP feature allows you to load balance outgoing traffic across all IGP ECMP paths proportionally to the interface bandwidth. |
| Configuring Dynamic ARP Inspection | Dynamic ARP Inspection (DAI) validates Address Resolution Protocol (ARP) packets in a network. With DAI, you can intercept, log, and discard ARP packets with invalid MAC address to IP address bindings. This capability protects the network from certain man-in-the-middle attacks. |
| Configuring EVPN VXLAN External Connectivity | You can configure the EVPN VXLAN external connectivity for enterprise routers. External connectivity refers to the movement of Layer 2 and Layer 3 traffic between an EVPN VXLAN network and an external network. This enables the EVPN VXLAN network to exchange routes with the externally connected network. |
| Configuring Interface Template | An interface template is a container of configurations or policies that can be applied to specific ports. This feature allows you to configure an IPV4 or IPv6 ACL in the interface template for the Cisco SM-X EtherSwitch module. |

| Feature | Description |
|---|---|
| Configuring IPv6 First Hop Security | The Switch Integrated Security Feature (SISF) based device tracking feature is part of the suit of first hop security features. This feature allows to track the presence, location, and movement of end-nodes in the network. The First Hop Security features are supported as a part of device tracking policy:<br>• Static IPv6Address Bind<br>• IPv6 Address Glean, Inspection, and Guard<br>• IPv6 Device Tracking<br>• IPv6 Binding Recovery |
| Configuring Per-Interface Per-Cause Punt Policer | The per-interface per-cause (PIPC) punt policing is an enhancement to the punt policing and monitoring feature that allows you to configure the limit on traffic per interface. Starting from the Cisco IOS XE 17.5.1 release, you can set the per-interface per-cause rate for all the control plane punted traffic. This rate causes any traffic beyond the set limit to be dropped, therefore allowing you to control the traffic during conditions such as L2 storming. |
| ISIS: Flex Algo: Support for Affinity Include any/all | Segment Routing Flexible Algorithm with IS-IS: Segment Routing Flexible Algorithm allows operators to customize IGP shortest path computation according to their own needs. An operator can assign custom SR prefix-SIDs to realize forwarding beyond link-cost-based SPF. As a result, Flexible Algorithm provides a traffic engineered path automatically computed by the IGP to any destination reachable by the IGP. This release also introduces support for the following functionalities:<br>• Flex Algo prefix metric: Flex-algo prefix-metric allows to associate metric computed in given flex-algo with a prefix during prefix inter-level leaking or during inter-domain redistribution .This help to compute optimal inter-level or inter-domain path Support for affinities include any/all: Ability to pick and choose the links that they want. User can use a certain path without creating a label stack by using the Prefix SIDs or Adjacency SIDs<br>• TI LFA + uLoop Avoidance: Allows computation of Loop Free Alternate (LFA) paths. TI-LFA backup paths using the same constraints as the calculation of the primary paths for Flexible Algorithms, for IS-IS Inter-area leaking of Flexible Algorithm SIDs and prefixes and selectively filtering the paths that are installed to the MFI are also supported. |
| Traffic Steering by Dropping Invalid Paths | If the SR-TE Policy has no valid paths defined, the paths are dropped and traffic being steered through the policy falls back to the default (unconstrained IGP) forwarding path. Also, when a SR-TE policy carrying best-effort traffic fails, traffic is re-routed and this impacts the SLA for premium traffic.To solve this issue, if the SR-TE policy fails, the traffic in the data plane is dropped but kept in the controlplane. Therefore, other SR policies, potentially carrying premium traffic, are not impacted. |
| Tunnel Path MTU discovery on MPLS-enabled GRE tunnel | You can now use the tunnel mpls-ip-only command to configure how the Do Not Fragment bit from the payload is copied into the tunnel packets IP header.If the Do Not Fragment bit is not set, the payload is fragmented if an IP packet exceeds the MTU set for the interface. |

| Feature | Description |
|---|---|
| View traffic counters for SR-TE policies | You can now view the traffic counters of SR-TE policies using the show segment-routing traffic-eng policy command. |
| Replicate inner IP's DF-bit over the Outer IP only for the GRE | You can now use the tunnel mpls-ip-only command to configure how the Do Not Fragment bit from the payload is copied into the tunnel packets IP header.If the Do Not Fragment bit is not set, the payload is fragmented if an IP packet exceeds the MTU set for the interface. |
| Dynamic Allocation of Cores | Cisco devices allow limited flexibility on how services run on the service plane cores. Dynamic core allocation allows in-service upgrade of services, which eliminates the inactivity of compute resources. Starting from Cisco IOS XE release17.5, the system does not require a reboot for the changes to take effect. |
| License Management for Smart Licensing Using Policy, Using Cisco vManage | Cisco SD-WAN operates together with Cisco SSM to provide license management through Cisco vManage for devices operating with Cisco SD-WAN. For this you have to implement a topology where Cisco vManage is connected to CSSM. For information about this topology, see the Connected to CSSM Through a Controller, and to know how to implement it, see the<br><br>Workflow for Topology: Connected to CSSM Through a Controller sections of the *Smart Licensing Using Policy for Cisco Enterprise Routing Platforms* guide.<br><br>For more information about Cisco vManage, see the License Management for Smart Licensing Using Policysection of the *Cisco SD-WAN Getting Start Guide*.<br><br>For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide. |

# Cisco Catalyst 8300 Series Edge Platforms ROMMON Compatibility Matrix

The following table lists the ROMMON releases supported in Cisco IOS XE 17.5.x releases.

***Table 2: Minimum and Recommended ROMMON Releases Supported on C8300-1N1S-4T2X|6T***

| Cisco IOS XE Release | Minimum ROMMON Release Supported for IOS XE | Recommended ROMMON Release Supported for IOS XE |
|---|---|---|
| 17.3.1 | 17.3(1r) | 17.3(1r) |

***Table 3: Minimum and Recommended ROMMON Releases Supported on C8300-2N2S-4T2X|6T***

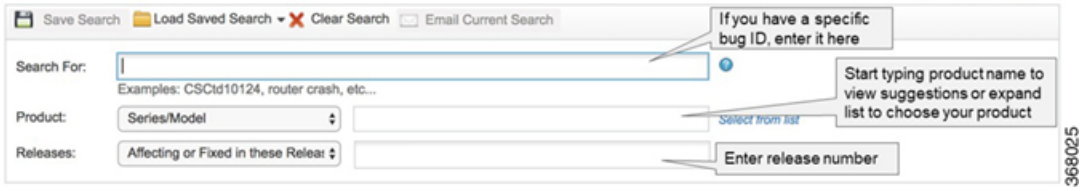
| Cisco IOS XE Release | Minimum ROMMON Release Supported for IOS XE | Recommended ROMMON Release Supported for IOS XE |
|---|---|---|
| 17.3.1 | 17.3(1.2r) | 17.3(1.2r) |

# Resolved and Open Bugs

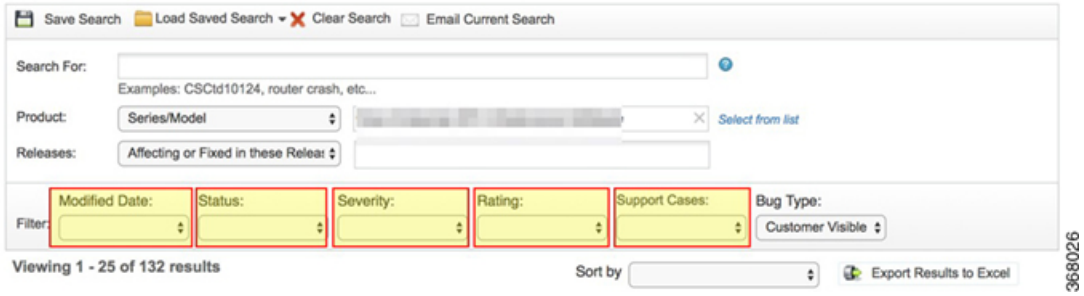
### About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.




You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.




## Resolved Caveats in Cisco IOS XE Bengaluru 17.5.1

| Caveat ID Number | Description |
|---|---|
| CSCvw33950 | Router reloads due to QFP STUCK-THREAD. |
| CSCvw43836 | Device crashed during the tunnel interface flap with jumbo frame. |
| CSCvw64452 | During Soak run, lot of policy drops due to less CPS rate set on the device. |
| CSCvu92655 | PIM-WP7601, RSSI MIB trap cannot be set to any LTE options |
| CSCvv44099 | PGE Flow Control can not be disable |
| CSCvw91925 | FHS Local entry stays down after configuring a SVI interface with same mac twice |

## Open Caveats in Cisco IOS XE Bengaluru 17.5.1

| Caveat ID Number | Description |
|---|---|
| CSCvw31389 | Device crashes when firewall logs contain subscriber names and the packet logging infrastructure attempts to display the summary record |

# Related Documentation

- Hardware Installation Guide for Catalyst 8300 Series Edge Platforms
- Policy for Smart Licensing guide
- Software Configuration Guide for Catalyst 8300 Series Edge Platforms