Release Notes for Cisco Catalyst 8000V Edge Software, Cisco IOS XE Bengaluru 17.4.x

First Published: 2020-12-18

Cisco Catalyst 8000V Edge Software Overview

About Cisco Catalyst 8000V

Cisco Catalyst 8000V Edge Software or Cisco Catalyst 8000V is a software-based, virtual router that combines the functionalities of Cisco Cloud Services Router (Cisco CSR1000V) and Cisco Integrated Services Virtual Router (Cisco ISRv) into a single image that is intended for deployment in on-prem branches, data centers, colocation data centers, and public clouds.

Cisco Catalyst 8000V supports NIM modules on Cisco ENCS platforms, runs on any x86 platform, and is supported on ESXi, KVM, and Cisco NFVIS hypervisors. Further, you can deploy this router on public cloud providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and Alibaba Cloud.

When you deploy Cisco Catalyst 8000V as a VM, the Cisco IOS XE software behaves similar to a traditional Cisco router (hardware platform). You can configure different features depending on the Cisco IOS XE software version.

Features

- **Hardware independence**: The Cisco Catalyst 8000V router uses the benefits of virtualization in the cloud to provide hardware independence. Since the Cisco Catalyst 8000V runs as a virtual machine, you can use this router on any x86 hardware that the virtualization platform supports.
- **Sharing of host hardware resources**: The host server hardware resources such as CPU cores, memory, and disk are managed by the hypervisor, and these resources are shared among the guest VMs. You can regulate the amount of hardware resources assigned to a specific Cisco Catalyst 8000V VM instance.
- **Flexibility in deployment**: You can easily move a VM from one server to another. Thus, you can move a Cisco Catalyst 8000V instance from a server in one physical location to a server in another physical location without moving any hardware resources.
- **Enhanced software security - Secure Object Store**: In Cisco Catalyst 8000V, storage partitions for NVRAM, licensing, and other data are created as object stores. The individual object stores are encrypted to ensure data security, and this product is Cisco Secure Development life cycle (CSDL) compliant. Further, Cisco Catalyst 8000V supports a 16G disk profile.

Hardware Requirements

For hardware requirements and installation instructions, see the Cisco Catalyst 8000V Edge Software Installation And Configuration Guide.

Software Images and Licenses

The following sections describe the licensing and software images for Cisco Catalyst 8000V.

Cisco Catalyst 8000V Software Licenses

The Cisco Catalyst 8000V is licensed based on throughput, feature-set, and the licensing term. This product supports Cisco Smart Licensing Usage Policy as well as Cisco DNA Licensing. Based on whether you want to opt for purchased licenses that go with the Cisco Catalyst 8000V instance, or a subscription-based license, choose one of the following options:

Subscription-Based Licensing via Cisco DNA

You can purchase a subscription license for Cisco Catalyst 8000V through the following licenses that are available via Cisco DNA:

- Cisco Catalyst 8000V - Network-Advantage
- Cisco Catalyst 8000V - Network-Essentials

For more information on Cisco Catalyst 8000V DNA licensing, see Cisco DNA Software for SD-Wan and Routing Ordering Guide.

Bring-Your-Own-Licensing

You also have an option to purchase and use licenses with Cisco Catalyst 8000V as a Bring-Your-Own-License (BYOL) instance or as a Pay-As-You-Go (PAYG) instance.

To use a Cisco Catalyst 8000V - BYOL license, see Licenses and Licensing Models to know to how install and configure your license.

If you have upgraded to Cisco Catalyst 8000V from a Cisco CSR 1000V or a Cisco ISRV, you must use Smart Licensing Using Policy (SLP). Traditional licenses do not work after the upgrade.

Pay-As-You-Go Licensing

Cisco Catalyst 8000V supports the PAYG Licensing model with Amazon Web Services (AWS) and Microsoft Azure Marketplace. Cisco Catalyst 8000V hourly-billed AMI or Pay As You Go licensing model allows you to consume an instance for a defined period of time. In this licensing model, you can directly launch the instance from the AWS or Azure Marketplace and start using the instances. The licenses are embedded in the image.

Note For demo or evaluation licenses, contact your Cisco Account Team if you have a direct purchase agreement with Cisco, or your Cisco Partner or Reseller.

For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

Software Image Nomenclature for Installation Files

The Cisco Catalyst 8000V installation file nomenclature indicates properties supported by the router in a given release.

For example, these are filename examples for the Cisco IOS XE Bengaluru 17.4.1a release:

- c8000v-universalk9.17.04.01a.ova
- c8000v-universalk9.17.04.01a.iso
- c8000v-universalk9.17.04.01a.qcow2

The following table lists the filename attributes along with its properties:

Table 1: Installation Filename Attributes

Filename Attribute	Properties
universalk9	Specifies the package that you are installing.
17.04.01a	Indicates that the software image is mapped to the Cisco IOS XE Bengaluru 17.4.1a release.

New and Enhanced Features for Cisco IOS XE Bengaluru 17.4.x

New and Enhanced Features for Cisco IOS XE Bengaluru 17.4.1

The following are the new Cisco Catalyst 8000V software features for Cisco IOS XE Bengaluru 17.4.1 release:

Note Starting from Cisco IOS XE 17.4.1, with the introduction of Smart Licensing Using Policy, even if you configure a hostname for a product instance or device, only the Unique Device Identifier (UDI) is displayed. This change in the display can be observed in all licensing utilities and user interfaces where the hostname was displayed in earlier releases. It does not affect any licensing functionality. There is no workaround for this limitation.

The licensing utilities and user interfaces that are affected by this limitation include only the following:

- Cisco Smart Software Manager (CSSM),
- Cisco Smart License Utility (CSLU), and
- Smart Software Manager On-Prem (SSM On-Prem).

- Smart Licensing Using Policy: An enhanced version of Smart Licensing with the overall objective of providing a licensing solution that does not interrupt the operations of your network but also enables a compliance relationship to account for the hardware and software licenses you purchase and use. With this licensing model, you do not have to complete any licensing-specific operations such as registering or generating keys before you start using the software and the licenses that are tied to it. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date.

Multiple options are available for license usage reporting which depends on the topology you implement. You can use the Cisco Smart Licensing Utility (CSLU) Windows application or report usage information directly to CSSM. A provision for offline reporting for air-gapped networks where you download usage information and upload to CSSM is also available. Starting with this release, Smart Licensing Using Policy is automatically enabled on the device. This is also the case when you upgrade to the current version of the release. By default, your Smart Account and Virtual Account in CSSM are enabled for Smart Licensing Using Policy.

For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

- Smart Software Manager On-Prem (SSM On-Prem) Support for Smart Licensing Using Policy: SSM On-Prem is an asset manager, which works in conjunction with CSSM. It enables you to administer products and licenses on your premises instead of having to directly connect to CSSM.

  Here, a product instance is connected to SSM On-Prem, and SSM On-Prem becomes the single point of interface with CSSM. The product instance can be configured to *push* the required information to SSM On-Prem. Alternatively, SSM On-Prem can be set-up to *pull* the required information from a product instance at a configurable frequency. After usage information is available in SSM On-Prem, you must synchronize the same with CSSM, to ensure that the product instance count, license count and license usage information is the same on both, CSSM and SSM On-Prem. Offline and online options are available for synchronization between CSSM and SSM On-Prem.

  Minimum Required SSM On-Prem Version: Version 8, Release 202102

  Minimum Required Cisco IOS XE Version: Cisco IOS XE Amsterdam 17.4.1

- Enhancements to Radio Aware Routing: Starting from the Cisco IOS XE 17.4.1 release, the following enhancement is available when you use the Radio-Aware-Routing feature with a Cisco Catalyst 8000V virtual router. Earlier, the RAR functionality used a credit-based mechanism to send data packets where each radio sent the data packets based on the credits. Now, a priority-based mechanism is first used to send the data packets. With this enhancement to the RAR functionality, the radio sends the data packets that are high priority first. This enhancement is auto-enabled, and no configuration changes are required.

- BGP Large Community: The BGP large communities support a routing policy to control the distribution of routing information. The BGP large communities attribute provides the capability of tagging routes and modifying BGP routing policy on the device. BGP large communities can be appended or removed selectively on the large community attribute as the route travels from device to device.

- NBAR Support on the EVC Service Instance: To classify the data packets, enable NBAR FIA-trace data for NBAR on the EFP interface. Quality of service (QoS) takes action on the output interface based on the NBAR traffic classification result.

- BGP-EVPNoMPLS Unknown Unicast Flooding Suppression: The unknown unicast flooding suppression feature provides the capability to block the unknown unicast traffic that are forwarded to the device. When the unknown unicast flooding suppression status is set to ON, the Control Plane Policing drops the packet with unicast destination MAC address.

- IP-SLA-HTTPS Support: This feature has enhanced capabilities of IP SLA device tracking with HTTPS probes and helps to verify reachability in the network.

  Configuring Stateless Static NAT: Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. A new keyword stateless is introduced for Cisco IOS XE static NAT configuration and it applies only to static NAT command. When the static mapping is set to stateless, no sessions will be created for that traffic flow.

- Configure Performance Measurement - This feature enables hardware timestamping. The Performance Measurement (PM) for link delay uses the light version of Two-Way Active Measurement Protocol (TWAMP) over IP and UDP.
- EPC support on LTE interface and FlexVPN interface: Embedded Packet Capture (EPC) is an onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from a device. This feature facilitates troubleshooting by gathering information about packet format.
- Configuring the Same Global Address for Static NAT and PAT: You can now configure the same global address within the static NAT and static PAT. This configuration is supported only on outside static NAT.
- The Web UI lets you configure the Smart Licensing on Cisco Catalyst 8000V. Further, you can monitor the Cellular Gateway. To learn more, refer to the WebUI Online Help.
- CUBE: Hunt Stop for Server Groups: Server groups allow you to create simpler configurations by specifying a list of destination SIP servers for a single dial peer. When a call matches a dial peer that is configured with a server group, the destination is selected from the list of candidates based on a configured policy. If it is not possible to complete that call, the next candidate is selected. Alternatively, you can also choose to stop hunting through the group if a specified response code is received. If the call cannot be placed to any of the servers in the group, or hunting is stopped, call processing continues to the next preferred dial-peer.
- CUBE: VoIP Trace Serviceability Framework: VoIP Trace is a Cisco Unified Border Element (CUBE) serviceability framework, which provides a binary trace facility for persistently monitoring and troubleshooting SIP call issues. The VoIP Trace framework records both successful and failed calls. All call trace data is stored in system memory. In addition, data for calls with IEC errors is written to the logging buffer.
- Unified SRST: Smart License Using Policy: Smart Licensing using Policy reports license usage periodically based on an account policy, rather than requesting licenses based on past usage as in previous releases. Evaluation mode and license reservation are not supported. License usage is reported to Smart Agent three minutes after the last configuration change. Now all the devices within a network follow the uniform approach of reporting their license usage to Smart Agent. The Smart Agent in turn creates a Resource Utilization Monitoring (RUM) report and dispatches to CSSM based on the Smart Agent reporting policy. See also https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide/enhanced_srst.html.

  For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.
- Unified CME: Smart License Using Policy: Smart Licensing using Policy reports license usage periodically based on an account policy, rather than requesting licenses based on past usage as in previous releases.Evaluation mode and license reservation are not supported. License usage is reported to Smart Agent three minutes after the last configuration change. Now all the devices within a network follow the uniform approach of reporting their license usage to Smart Agent. The Smart Agent in turn creates a Resource Utilization Monitoring (RUM) report and dispatches to CSSM based on the Smart Agent reporting policy.

  For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.
- CUBE: Smart License Using Policy: Smart Licensing using Policy reports license usage periodically based on an account policy, rather than requesting licenses based on past usage as in previous releases. Evaluation mode and license reservation are not supported. Frequent license requests used to go out from a device to CSSM in earlier versions. In the changed scenario, minimum reporting license usage is 8 hours. Now all the devices within a network follow the uniform approach of reporting their license usage

to Smart Agent. The Smart Agent in turn creates a Resource Utilization Monitoring (RUM) report and dispatches to CSSM based on the Smart Agent reporting policy.

For a more detailed overview on Cisco Licensing, go to https://cisco.com/go/licensingguide.

- CUBE: Clear Hung RTP Ports: When establishing a call, CUBE allocates several RTP ports that are based on the media that are negotiated for the session. Some ports remain assigned even after the call ends. In the current behavior, show voip rtp stats command displays only the ports allocated from the global table, even if the ports are allocated from all the three tables (Global port, media IP address-based, and media VRF-based). Now this command is enhanced to display the ports allocated from all the three tables. The command also displays the hung ports and allows you to release those ports. Releasing the hung ports increases the efficiency of the routers as more ports are available to receive calls.

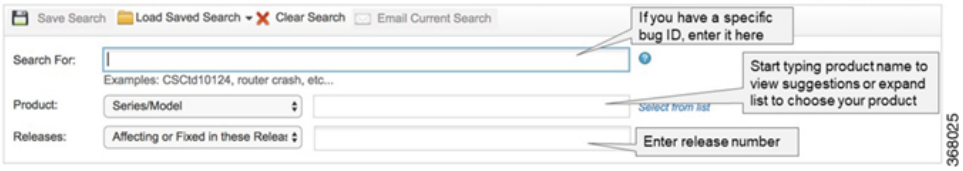
Resolved and Open Bugs for Cisco IOS XE Bengaluru 17.4.x

Using the Cisco Bug Search Tool

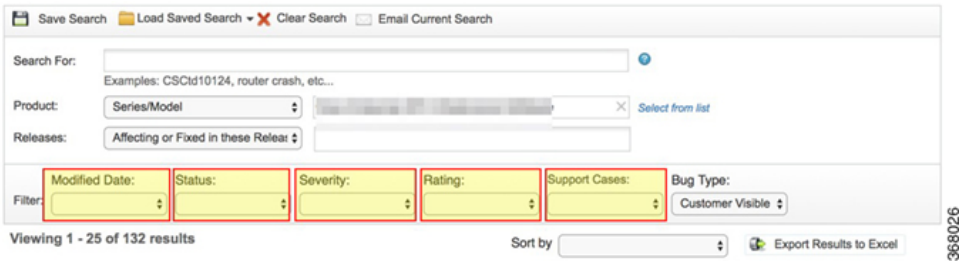
About the Cisco Bug Search Tool

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 the bugs specific to a product and a release.



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



Open Bugs for Cisco IOS XE Bengaluru 17.4.2

Caveat ID Number	Description
CSCvw84883	DDNS feature triggers crash on 16.X/17.X releases due to memory corruption

Resolved Bugs for Cisco IOS XE Bengaluru 17.4.2

Caveat ID Number	Description
CSCvw93490	CSR1000v crashing frequently with Critical software exception error.

Open Bugs for Cisco IOS XE Bengaluru 17.4.1

Caveat ID Number	Description
CSCvv38068	C8000v not booting up in Azure if assigned IPaddr 10.0.1.0 to Gig1 Interface
CSCvv38068	C8000v not booting up in Azure if assigned IPaddr 10.0.1.0 to Gig1 Interface
CSCvy02029	C8000V new PAYG Azure Cloud deployments do not boot with correct throughput level and tech package
CSCvt58920	SIM failover within the same modem takes long time to detect LTE network for AT&T
CSCvv23293	GreenDay: With router reload Breakout 10g port Te0/2/1 is down due to remote fault.
CSCvv33576	IGMP snooping table not populated
CSCvv44331	AppQoe Clear Alarm is not generated from device
CSCvv79072	25G license tags is retained and throughput throttled after upgrade from 17.3.1 to 17.3.2
CSCvv84400	IR1101 - WP7607 modem is changing to down state after ping to enodeB
CSCvv88621	GETVPN: All GM will crash when Primary KS recovers its COOP role after network outage
CSCvv94743	Data Plane fails over L2TPv3 while disabling VLAN limit restrictions with ASR1002-HX
CSCvw11902	Passive FTP doesn't work with NAT
CSCvw13048	crash observed at NHRP while using summary-map
CSCvw33113	Unexpected reload in NHRP when access to an invalid memory region
CSCvw34157	APPNAV CFT Crashes
CSCvw36629	cEdge: NATed tuple flips for HSL deleted flow
CSCvw39383	CPP ucode crash with fw_base_flow_create
CSCvw47640	KS role for GETVPN is sending malformed rekey packets
CSCvw47800	HSL Export over VASI Interface causes Netflow v9 Template Flooding
CSCvw48800	unable to transfer 1500 byte IP packet when using BRI bundled Multilink
CSCvw48943	crypto ikev2 proposals are not processed separately

Caveat ID Number	Description
CSCvw54076	[SIT]: BFD sessions not established between Edges, with UTD enabled
CSCvw58560	FlexVPN reactivate primary peer feature does not work with secondary peer tracking
CSCvw70009	Fman_rp crash seen on 16.9.X when "show platform software nat RP active logging" is run
CSCvw70461	17.4 ZBFW:Classification of traffic not happening correctly sometimes when a rule in RS is edited.
CSCvw71941	QFP crash in cpp_ess_tc_tgt_if_fm_edit_helper
CSCvw73701	17.4 ZBFW:Stale ACL entries seen
CSCvw74781	C1111 ARP resolution failure after shut/no shut operation
CSCvw74921	APPNAV CFT crash
CSCvx86151	ovf-template should give option for DNA essentials, advantage, premier on C8kv deployment in vcenter

Resolved Bugs for Cisco IOS XE Bengaluru 17.4.1

Caveat ID Number	Description
CSCvv25529	16.12.4 ucmk9 cedge not able to join overlay with 19.2.3 and 20.3
CSCvv14438	Azure csr-cedge 17.3.1 fresh deploy crash once@qfp-ucode-csr when shut/no-shut Gi1
CSCuv97577	Mishandling of dsmpSession pointer causes a crash
CSCvt53843	ucode crash on ESP-100 with CAPWAP traffic when CAPWAP stripping is enabled
CSCvt89441	IOS-XE device crashed with CGD shared memory corruption freed by FMAN-FP
CSCvu07639	UTD policy on global VPN does not work properly for DIA traffic
CSCvu10006	Performance monitor caused QoS miss classification
CSCvu11066	Umbrella custom dns config not in sync between confd and ios
CSCvu11115	IOS-XE MTP Fails to Interwork DTMF RFC2833 from Payload 100 to Payload 101
CSCvu27953	Crash due to a segmentation fault in the "IPsec background proc" process
CSCvu34009	Calls going through T1 are rejected with "no dsps found" Analog/TDM Hairpin calls
CSCvu34381	Packets are not dropped as expected in selfzone to zone vpn 0 firewall config
CSCvu43248	%IP-4-DUPADDR: Duplicate address issue at NAT-HSRP router

Caveat ID Number	Description
CSCvu65669	Traffic drop from branch overlay ping to service side without zp vpn1 to vpn1 when FW & IPS enabled
CSCvu76378	Curie : DP_Stuck is observed after reloading the NIM-VA-B module overnight
CSCvu77745	PMAN-3-PROCFAIL: Chassis 1 R0/0: pman: R0/0: The process keyman has failed (rc 139)
CSCvu89033	Template push error due to NAT-MIB process helper traceback/warm restart
CSCvv03229	Crash in sre_dp_traverse_dfa_legacy as SIP invite messages crosses a GRE Tunnel
CSCvv04236	IOS-XE: IPv6 OSPF authentication ipsec - adjacency fails
CSCvv08341	Netconf deleting wrong IKEv2 parameters
CSCvv12401	ZBFW HA redundancy stuck in STANDBY-COLK-BULK. Bulksync Traceback seen in logs
CSCvv20380	Removing and Adding Bulk ACL leads to Tracebacks and Error-Objects
CSCvv26538	Crash due to a NULL pointer while bringing down PPPoE sessions.
CSCvv36247	Memory Leak in MallocLite / Crypto IKMP
CSCvv47691	Reload: IOS-XE router crashing due to DN mismatch
CSCvv58312	17.4 : Dataplane Crash due to driver cpp_drv_i95_read_cb observed on 4461 with traffic
CSCvv79273	Router may crash when using Stateful NAT64
CSCvv82330	When large number of policies are applied to the device running 17.3.1, traffic is dropped.
CSCvv83345	Summary/default-map routes getting ignored for p2p interface
CSCvw06719	"platform ipsec reassemble transit" tail-drops unencrypted IPv4 Fragments with specific payload
CSCvw56517	LMR Unable to hear first seconds of audio

Related Documentation

Cisco Catalyst 8000V Edge Software Product Page

Cisco Catalyst 8000V Edge Software Data Sheet

Cisco Catalyst 8000V Edge Software Installation And Configuration Guide

Cisco Catalyst 8000V Edge Software High Availability Configuration Guide

Troubleshooting Guide for Cisco Catalyst 8000V Edge Software

Smart Licensing Using Policy for Cisco Enterprise Routing Platforms