Release Notes for Cisco Catalyst 8000V Edge Software, Cisco IOS XE Dublin 17.11.x

First Published: 2023-04-06

Full Cisco Trademarks with Software License

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 cloud and virtual data centers.

Cisco Catalyst 8000V supports NIM modules, runs on any x86 platform, and is supported on ESXi, KVM, 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 on a VM, the Cisco IOS XE software functions as if it were deployed on a traditional Cisco hardware platform. You can configure different features depending on the Cisco IOS XE software image.

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 on a virtual machine, you can use this router on any x86 hardware that the virtualization platform supports.
- **Sharing of resources**: The resources used by Cisco Catalyst 8000V are managed by the hypervisor, and these resources can be shared among the VMs. You can regulate the amount of hardware resources that the VM server allocates to a specific VM. You can reallocate resources to another VM on the server.
- **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 cycle 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 go 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 three licenses that are available via Cisco DNA:

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

For more information on Cisco Catalyst 8000V DNA licensing, see Cisco DNA Software Routing Subscription 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 Dublin 17.11.1a release:

- c8000v-universalk9.17.11.01a.ova
- c8000v-universalk9.17.11.01a.iso
- c8000v-universalk9.17.11.01a.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.
17.11.01a	Indicates that the software image is mapped to the Cisco IOS XE Dublin 17.11.1a release.

Product Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround or other user action. For more information, see https://www.cisco.com/c/en/us/support/web/field-notice-overview.html.

We recommend that you review the field notices to determine whether your software or hardware platforms are affected. You can access the field notices from https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html#%7Etab-product-categories.

New and Enhanced Features for Cisco IOS XE Dublin 17.11.x

New and Enhanced Features for Cisco IOS XE 17.11.1a

Table 2: Software Features

Feature	Description
Attaching Extended Color Communities to BGP VRF	This feature introduces new methods of attaching extended color communities to a prefix. A color community is an indicator of the bandwidth or latency level of the traffic sent to the prefix. You can attach the the extended color communities to the prefix in the following ways: VRF export coloring, VRF import coloring, Route Redistribution coloring into BGP and Neighbor inbound coloring.
Bridge Domain VIF Support on Layer 2 EVPN	This enhancement allows configuring a Layer 2 EVPN network to support a Bridge Domain Interface (BDI) to act as an interface to a routing domain. Also, you can attach one or more bridge domain VIF interfaces to an EVPN Layer 2 network.

Feature	Description
Device Telemetry	This functionality enables collection of anonymous usage telemetry data for Cisco products, which helps in continuous product improvements. From Cisco IOS XE 17.11.1a, this functionality is enabled by default.
Deprecation of Weak Ciphers	The minimum Rivest, Shamir, and Adleman (RSA) key pair size must be 2048 bits. The compliance shield on the device must be disabled using the **crypto engine compliance shield disable** command to use the weak RSA key.
MAC and IP Addressing Learning from a Static ARP Alias Entry	This enhancement allows you to configure an EVPN VXLAN network to learn an EVPN MAC address and IP binding from a static Address Resolution Protocol (ARP) alias entry. After learning the MAC address and IP binding, an EVPN Type-2 route is advertised across the EVPN network.
Quantum-Safe Encryption Using Post-Quantum Preshared Keys	This feature implements RFC 8784 and Cisco Secure Key Integration Protocol (SKIP) for quantum-safe encryption of IKEv2 and IPsec packets using Post-quantum Preshared Key (PPK). The PPKs configured manually are referred to as manual PPKs and the PPKs imported from an external key source (KS) using the SKIP protocol are referred to as dynamic PPKs. This feature is applicable to all IKEv2/IPsec VPNs such as FlexVPN (SVTI-DVTI) and DMVPN, except for GETVPN. For more information, see the Cisco IOS Security Command Reference guide.
Redirecting Deprecated LISP Commands to Revised Versions	The feature includes a list of deprecated LISP commands which will automatically redirect the user to the updated command and associated output when executed. A banner will appear on the screen to notify the user that the previous command has been replaced. No functionality changes have been made to the revised commands.
Replication of Broadcast, Unknown-unicast, and Multicast Traffic	With this enhancement, the multi-destination Layer 2 broadcast, unknown-unicast, and multicast (BUM) traffic in an EVPN VXLAN network is replicated through a multicast group in the underlay network and forwarded to all the endpoints of the network.
Support for RAR PPPoE IPv6 Multicast	This feature provides support for IPv6 multicast in PPPoE-based Radio Aware Routing (RAR) networks.
Support for 16 vCPU in KVM	Cisco Catalyst 8000V now supports 16 vCPU instances in a KVM environment.

Table 3: Cisco Unified Border Element (CUBE) Features

Feature	Description
Unified SRST: Concurrent use of Webex Calling Survivability Gateway and Unified SRST	From Cisco IOS XE 17.11.1a, concurrent use of Cisco Webex Calling Survivability Gateway and Unified SRST is supported on the same router.

Table 4: Smart Licensing Using Policy Features

Feature	Description
Snapshots for Product Activation Key (PAK) licenses	Starting with Cisco IOS XE Dublin 17.11.1a, the PAK-managing library is discontinued and the provision to *take* a snapshot is no longer available. Software images from Cisco IOS XE Dublin 17.11.1a onwards rely only on the snapshotted information about PAK licenses. For more information, see: Snapshots for PAK Licenses. If you have a PAK license without a snapshot, and you want to upgrade to Cisco IOS XE Dublin 17.11.1a or a later release, you will have to upgrade twice. First upgrade to one of the releases where the system can take a snapshot of the PAK license and complete DLC, and then again upgrade to the required, later release.

Resolved and Open Bugs - Cisco IOS XE 17.11.x

Resolved Bugs - Cisco IOS XE 17.11.1a

Bug ID	Headline
CSCwe19394	Device may boot up into prev_packages.conf due to power outage
CSCwc99038	C8000V stuck in Day-0 prompt with the customdata having invalid syntax
CSCwd62953	C8000V : error platform provided UDI list has invalid values: ; udi_sn is empty
CSCwe37002	C8000V does not accept two file formats during day 0 configuration in OpenStack
CSCwe09916	QoS shaping parameter range is shown in [8000-10000000000] (only up to 10G)
CSCwd47940	PMTU Discovery is not working after interface flap
CSCwd45402	MSR Unicast-To-Multicast does not work if DST and SRC are the same in the service reflect configuration
CSCwc79115	Device policy commit failure notification and alarm from vsmart
CSCwd16559	ISG FFR: ARP request to reroute nexthop IP is not triggered if ARP entry not in ARP table
CSCwe28204	Control connection over L3 Tloc extension failing as no NAT table entry created
CSCwe34808	FMAN FP leak due to the punt-policer command

Bug ID	Headline
CSCwe09805	OID for SNMP monitoring of DSP resources are not working as expected
CSCwd89012	Tested flap-based auto-suspension - minimum duration value - no results as expected
CSCwe29430	Critical process fpmd fault on rp_0_0 (rc=134)
CSCwd87195	NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support.
CSCwd81357	QoS Classification does not work for DSCP or ACL + MPLS EXP
CSCwc99823	Fman crash seen in SGACL@ fman_sgacl_calloc
CSCwd90168	Unexpected reload after running the **show voice dsp** command while an ISDN call disconnects
CSCwd44439	Device crashes at fman_sdwan_nh_indirect_delete_from_hash_table
CSCwd34941	NAT configuration with no-alias option is not preserved after reload
CSCwc72588	Router does not allow weak cryptographic algorithms to be configured for IPsec
CSCwd25107	Interface VLAN1 placed in "shutdown" state when configured with "ip address pool"
CSCwc68069	RTP packets are not forwarded when packet duplication is enabled. No issue without duplication feature
CSCwe00946	System crash after disabling endpoint-tracker on tunnel interfaces
CSCwe18058	Unexpected reload with IPS is configured
CSCwd61255	Data Plane Crash on the device when Making Per-Tunnel QoS configuration changes with scale
CSCwe01015	IKEv2/IPSec - phase 2 rekey fails when peer is behind NAT
CSCwd17272	UTD Packet drops due to fragmentation for ER-SPAN traffic
CSCwe27241	NBAR classification error with custom app-aware routing policy
CSCwc37465	Unable to push "no-alias" option on static NAT mapping from the management system
CSCwc67625	OU field is deprecated from CA/B Forum Certificate Authorities
CSCwc65697	Device crashes and restarts during call flow
CSCwd44006	Control connection on the device doesn't come-up with reverse proxy using Enterprise Certificate
CSCwe23276	Change in the IPsec integrity parameters breaks the connectivity
CSCwd46921	Device does not connect to second vSmart after both the assigned vSmart are down
CSCwd12330	Invalid TCP checksum in SYN flag packets passing through Router
CSCwd30578	Wired guest client stuck at IP_LEARN with dhcp packets not forwarded out of the foreign to anchor
CSCwe33793	Memory allocation failure with extended antireplay enabled
CSCwd15487	[MBPL Integration] kernel crash is observed when modem-power-cycle is executed
CSCwd67654	Fnf stats are getting populated with unknown in egress/ingress interface in vpn0

Bug ID	Headline
CSCwd38943	GETVPN: KS reject registration from a public IP
CSCwb59113	Device control and bfd session gets nat translated with static ip over Dialer interface
CSCwe03614	CWMP : MAC address of ATM interface is not included in the inform message
CSCwb46968	Device template attachment causes PPPoE commands to be removed from ethernet interface
CSCwe19084	NAT: Traffic is not translated to the same global address though PAP is configured.
CSCwd71586	BFD sessions flapping on an interface with SYMNAT may lead to IPSec crash
CSCwe41946	DTMF fails through IOS MTP during call on-hold
CSCwd85580	Unexpected reload after **set ospfv3 authentication null** command
CSCwd65945	LR Interface which has NAT enabled is chosen for webex traffic
CSCwd06923	Stale IP alias left after NAT statement is removed
CSCwc48427	BFD issues with clear_omp -> non-PWK + non-VRRP scenario only
CSCwd28593	Control connection flap of assigned device
CSCwe60059	Crash when using dial-peer groups with STCAPP
CSCwe32862	Router IOS-XE crash while executing AES crypto functions
CSCwe25076	ALG breaks NBAR recognition impacting application firewall performance.
CSCwd68994	ISAKMP profile doesn't match as per configured certificate maps
CSCwd79572	FW policy with app-family rule with FQDN causes traffic drop for other sequences
CSCwe91988	Need to disable CSDL compliance check for NPE images

Open Bugs - Cisco IOS XE 17.11.1a

Bug ID	Headline
CSCwe40024	98% memory utilization for C8000V
CSCwd07580	Azure: C8000V QFP uCode crash due to MLX4 driver
CSCwd97676	VMware C8000V 'show interfaces' counters are incorrect and display extremely large values
CSCwd42523	Same label is assigned to different VRFs
CSCwd45508	Device does not form BFD across serial link during upgrade
CSCwe52971	Bfd tunnels via Starlink remain in down state
CSCwe54089	ZTP process does not work
CSCwe37123	Device uses excessive memory when configuring ACLs with large object groups
CSCwe19394	Device may boot up into prev_packages.conf due to power outage
CSCwe18276	Route-map not getting effect when its applied in OMP for BGP routes
CSCwd68111	Device object group called in ZBFW gives error after upgrade

Bug ID	Headline
CSCwe49684	BFD sessions keep flapping intermittently

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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Troubleshooting

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at https://www.cisco.com/en/US/support/index.html.

Go to **Products by Category** and choose your product from the list, or enter the name of your product. Look under **Troubleshoot and Alerts** to find information for the issue that you are experiencing.