# Release Notes for Cisco Catalyst 8000V Edge Software, Cisco IOS XE 17.15.x

**First Published:** 2024-08-27

## 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 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, 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 three 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 17.15.1a release:

- c8000v-universalk9.17.15.01a.ova

- c8000v-universalk9.17.15.01a.iso
- c8000v-universalk9.17.15.01a.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. Images with the universalk9 designation in the image name refers to a universal image that offers all the Cisco IOS features including strong payload cryptography features such as IPSec VPN, SSL VPN, and Secure Unified Communications. This image also supports security features like Zone-Based Firewall and intrusion prevention. |
| 17.15.01a | Indicates that the software image is mapped to the Cisco IOS XE 17.15.1a 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 17.15.x

## New and Enhanced Software Features in Cisco IOS XE 17.15.1

**Note** Cisco IOS XE 17.15.1a is the first release for Cisco Catalyst 8000V in the Cisco IOS XE 17.15.x release series.

*Table 2: Software Features*

| Feature | Description |
|---|---|
| Support for AWS Local Zones | AWS Local Zones (LZs) enable you to deploy latency sensitive applications closer to end-users. Starting with Cisco IOS XE 17.15.1a, you can deploy Cisco Catalyst 8000V on c5d.2xlarge instances available in AWS Local Zones. |
| Support for Interface speed setting of 40000 | From Cisco IOS XE 17.15.1a, you can set an interface speed of upto 40000 in Cisco Catalyst 8000V. This enables some traffic profiles to see higher throughputs. |
| Support for RHEL 9.2 hypervisor for KVM hosts | From Cisco IOS XE 17.15.1a, you can deploy Cisco Catalyst 8000V on RedHat RHEL 9.2 operating system with KVM hypervisor.<br>Note that support for RHEL 7.x is deprecated from this release. |
| Support for SUSE Linux® Enterprise Server 15 SP5 | From Cisco IOS XE 17.15.1a, you can deploy Cisco Catalyst 8000V on SUSE Linux® Enterprise Server 15 SP5 operating system with KVM hypervisor. |
| Support for VMware ESXi 8.0 | From Cisco IOS XE 17.15.1a, you can deploy Cisco Catalyst 8000V on VMware ESXi 8.0 Update 2 hypervisor operating system.<br>Note that ESXi hypervisor version 6.0 will no longer be supported from this release. |
| Absolute Path for HTTP or HTTPS File Transfer | The File Transfer using HTTP or HTTPs feature allows you to copy files from a remote server to your local device, using the **copy** command. From Cisco IOS XE 17.15.1a, you must provide the absolute file path when you execute the **copy** command, to transfer the file. |
| Cisco Umbrella Scope Credentials | From Cisco IOS XE 17.15.1a, this feature provides the ability to define and configure a new single Cisco Umbrella credential for both Umbrella SIG and Umbrella DNS. |
| Configure DMVPN for SD-Routing Devices | Cisco DMVPN (Dynamic Multipoint VPN) is a routing technique to build a VPN network with multiple sites without having to statically configure all devices. This technique uses tunnelling protocols and encrypted security measures to create virtual connections, or tunnels, between sites. These tunnels are dynamically created as needed, making them both efficient and cost-effective. |

| Feature | Description |
|---|---|
| Configure Multiple WAN Interfaces on Cisco SD-Routing Devices Using a Custom VRF | You can now create a custom VRF that hosts one or more WAN interfaces. You can extend this functionality to create multiple custom VRFs with each VRF hosting multiple WAN interfaces. These WAN interfaces now function as transport interfaces to establish control connections to the Cisco Catalyst SD-WAN Manager. Having multiple WAN interfaces ensures that there is resiliency in control connections and routing of transport traffic. |
| Configure Site-Cloud Support to AWS Using Configuration Groups | This release introduces support to configure site to cloud connectivity from an SD-Routing branch to Amazon Web Services using Configuration Groups. This is an enhancement over the existing implementation of configuring site to cloud connectivity from an SD-Routing branch to Amazon Web Services using CLI-Add on Profile. |
| Enabling Flow Level Flexible NetFlow Support for SD-Routing Devices | The Flow-level Flexible NetFlow (FNF) feature allows you to monitor the NetFlow traffic and view all the flow-level FNF data that is captured including application-level statistics. |
| Enhanced NAT Management | From Cisco IOS XE 17.15.1a, the Enhanced NAT Management feature enables network operators to safeguard system performance by limiting NAT translations based on CPU usage with the ip nat translation max-entries cpu command. This feature also enables streamlining NAT synchronization in redundant systems using the **ip nat settings redundancy optimized-data-sync** command. |
| Enhancements to Segment Routing over IPv6 Dataplane | From Cisco IOS XE 17.15.1a, Segment Routing over IPv6 dataplane supports these functionalities:<br>• IS-IS Microloop Avoidance<br>• IS-IS Loop-Free Alternate Fast Reroute<br>• IS-IS Topology-Independent Loop-Free Alternate Fast Reroute<br>• OAM Traffic Engineering |
| Monitoring Software Defined (SD) - Routing Alarms | From Cisco IOS XE 17.15.1a, network administrators can monitor SD-Routing device alarms on Cisco Catalyst SD-WAN Manager. This feature enables SD-Routing devices to record and store various alarms generated by control components and routers. For more information, see Cisco SD-Routing Command Reference Guide. |

| Feature | Description |
|---|---|
| Network-Wide Path Insights on Software Defined (SD) - Routing Devices | Network-Wide Path Insights (NWPI) is a tool that allows network administrators to monitor Cisco SD-Routing deployment, identify network and application issues, and optimize the network. |
| SD-Routing License Management | This release introduces license management support for SD-Routing devices. The supported licensing workflows include license assignment or configuration, license use, and license usage reporting. Depending on the device, these workflows are performed in the Cisco Catalyst SD-WAN Manager or on the device. |

# Resolved and Open Bugs - Cisco IOS XE 17.15.x

## Resolved Bugs - Cisco IOS XE 17.15.1a

| Identifier | Headline |
|---|---|
| CSCwi90648 | C8000v crashes in ESXi On-prem environment |
| CSCwi34858 | NETVSC VLAN sub interfaces not passing traffic after upgrade |
| CSCwj85529 | C8000V license boot level config done via 'customdata' is getting lost after reload |
| CSCwk54698 | C8000V hosted in Azure reloaded unexpectedly generating a system report |
| CSCwj51700 | CPP crashes after re-/configuring **ip nat settings pap limit ... bpa** feature in high QFP state. |
| CSCwk42634 | %PMAN-0-PROCFAILCRIT: R0/0: pvp: A critical process vip_confd_startup_sh has failed (rc 6) |
| CSCwk33173 | EzPM application-performance profile cause memory leak and crash with long-lived idle TCP flows. |
| CSCwk16333 | Device repeatedly crashing in FTMd due to FNF flow add. |
| CSCwj96852 | Return traffic for outside to inside NAT traffic received on one TLOC is forwarded out of other TLOC. |
| CSCwj95633 | SAIE application - no data to display for IOS XE router. |
| CSCwk39131 | Device crashed when issuing **show sdwan ftm next-hop chain all**. |
| CSCwk22225 | FTMd crashes after receiving credentials feature template update. |
| CSCwj48909 | Coredump observed in tracker module while running cxp_sig_auto_tunnel suite. |
| CSCwk45165 | fman_fp memory leak on device. |

| Identifier | Headline |
|---|---|
| CSCwj84949 | Unencrypted traffic due to non-functional IPsec tunnel in FLEXVPN hub & spoke setup. |
| CSCwj90614 | High CPU utilisation for confd_cli. |
| CSCwi81026 | BFD sessions flapping during IPSec rekey in scaled environment. |
| CSCwk39268 | sdn-network-infra-iwan failing to renew with "hash sha256" > 17.11. |
| CSCwj76662 | High memory utilization due to "ftmd" process. |
| CSCwk31715 | After deleting a NAT configuration, the IP address still shows up in routing table. |
| CSCwk12524 | Device reloaded due to ezManage mobile app service. |
| CSCwk44078 | GETVPN / migrating to new KEK RSA key does not trigger GM re-registration. |
| CSCwk22942 | Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other. |
| CSCwj96092 | ICMP tracker type (from echo to timestamp) change causes tracker to fail. |
| CSCwj99827 | Device unexpectedly reloads due to a crash in 'vdaemon' process. |
| CSCwi99454 | FNF test_tunnel_name_change_CSCvt57024 case failed due to session of pm5 was not alive. |
| CSCwj40223 | appRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns wrong order. |
| CSCwj02401 | Router reloaded when generating admin tech while processing very high number of flows. |
| CSCwk19725 | add FNF cache limit for show sdwan app-fwd flows. |
| CSCwj86794 | Device crashes while processing an NWPI trace. |
| CSCwk42253 | Unexpected reboot when a HTTP connection failed with 404 on a controller mode router. |
| CSCwj67591 | Chassis activate effective only after second re-try - with new uuid. |
| CSCwj32347 | DIA endpoint tracker not working with ECMP routes. |

## Open Bugs - Cisco IOS XE 17.15.1a

| Identifier | Headline |
|---|---|
| CSCwh91039 | C8000V: High system CPU load reported due to unsupported number of vCPUs allocated |
| CSCwk75733 | Custom applications may not be programmed properly. |

| Identifier | Headline |
|---|---|
| CSCwk89256 | Speed mismatch in IOS-XE configuration after device template push. |
| CSCwk85704 | "match traffic-category " add-on CLI push failed. |
| CSCwk87944 | VRRP switchover with tloc preference change is generating rekey and crypto add/delete events. |
| CSCwk86355 | File transfer fails "lost connection". |
| CSCwk49806 | Router rebooted unexpectedly due to process NHRP crash. |
| CSCwk81360 | Router can reboot unexpectedly while configuring NAT static translation. |
| CSCwk62954 | Multiple "match address local interface <int>" not pushed under crypto profile. |
| CSCwk63722 | Startup configuration failure post PKI server enablement. |
| CSCwm07564 | data-policy local-tloc-list breaks RTP media stream. |
| CSCwk54544 | ZBFW TCAM misprogramming after rules are reordered. |
| CSCwk74298 | Device denied for template push and some show commands with error application communication failure. |
| CSCwk98578 | GETVPN IPv6 crypto map not shown in interface configuration. |
| CSCwj05500 | Accelerated networking stops working due to driver issue. |
| CSCwk70630 | Cannot import device certificate. |
| CSCwk97930 | Crash occurs when IPv6 packets with link-local source are forwarded to SDWAN tunnels. |
| CSCwm13223 | Device crashes in IOSd due to malformed DMVPN-5-NHRP_RES_REPLY_IGNORE syslog. |
| CSCwk79454 | Endpoint tracker does not fail if default route is removed. |
| CSCwk69597 | C8000V running config write memory did not persist after reload. |
| CSCwk90014 | NAT DIA traffic getting dropped due to port allocation failure. |
| CSCwi87546 | Device unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - lock id of 0 released. |
| CSCwk61238 | RRI static not populating route after reload if stateful IPSec is configured. |
| CSCwm12851 | Device uses 3DES as default rekey algorithm for GETVPN. |
| CSCwk95044 | 1SPA.smu.bin drops when packet duplication link fails-over. |
| CSCwj87028 | Device showing custom APP as "unknown" for egress traffic when using DRE Opt. |
| CSCwm08545 | Centralized policy policer worked per PC on the same site not per site/vpn-list. |

| Identifier | Headline |
|---|---|
| CSCwf62943 | System image file is not set to packages.conf when image expansion fails due to disk space. |
| CSCwm00309 | Packets not hitting the correct data policy after modifying the action of a sequence. |

# 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 DevNet.
- 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.