Release Notes for Cisco Catalyst 8000V Edge Software, Cisco IOS XE 17.14.x

First Published: 2024-04-30

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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/c/en/us/about/

legal/trademarks.html. 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)

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 17.14.1a release:

- c8000v-universalk9.17.14.01a.ova

- c8000v-universalk9.17.14.01a.iso
- c8000v-universalk9.17.14.01a.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, Intrusion Prevention through the SECNPE-K9 license.
17.14.01a	Indicates that the software image is mapped to the Cisco IOS XE 17.14.1a 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 17.14.x

New and Enhanced Software Features in Cisco IOS XE 17.14.1a

Note Cisco IOS XE 17.14.1a is the first release for Cisco Catalyst 8000V in the Cisco IOS XE 17.14.x release series.

Table 2: Software Features

Feature	Description
AWS Migration Tool	From Cisco IOS XE 17.14.1a, an AWS migration tool is available as a CloudFormation template, to migrate your AWS instances from Cisco CSR1000V to Cisco Catalyst 8000V. This one-click solution consolidates and automates the migration process for a seamless migration experience, and is available in the AWS Marketplace.
Configuration Group Enhancements	This release introduces support for the following in Cisco SD-WAN Manager: • Transport Profiles • Management Profile • Service Profile • CLI Profile • Policy Object Profile
Configure Secure Service Edge	Secure Service Edge is a cloud solution that provides seamless, transparent, and secure Direct Internet Access (DIA) to protect against internet-based threats. This solution can be configured through Policy Groups by using Cisco SD-WAN Manager
Configure SSL/TLS Proxy for Decryption of TLS Traffic on SD-Routing Devices	The SSL/TLS Proxy feature allows you to configure an autonomous device as a transparent SSL/TLS proxy. Such proxy devices can then decrypt incoming and outgoing TLS traffic to enable their inspection by Unified Threat Defense (UTD) and identify risks that are hidden by end- to-end encryption.
View Unmodelled Commands on SD-Routing Devices	After an SD-Routing device is deployed, you can view the unmodelled commands on Cisco SD-WAN Manager. The list of unmodelled commands are regenerated if the device reboots

Feature	Description
YANG Configurational Model Support for SD-Routing Devices	This release introduces support for the following YANG Configurational Models: • BGP • MPLS • RSVP • SNMP • AAA • QOS • ACL • DHCP
Support to Configure VPN Solutions for SD-Routing devices	This release introduces support for the following VPN solutions: • FlexVPN • GETVPN • DMVPN • L3VPN These VPN solutions can be configured by using **Configuration** > **Configuration Groups** > **CLI Add-on Profile** option in Cisco SD-WAN Manager.
Enhanced IS-IS Fast Flooding	The IS-IS Fast Flooding feature optimizes LSP transmission to accelerate network convergence by dynamically adjusting the LSP rate based on receiver capability. From Cisco IOS XE 17.14.1a, IS-IS Fast Flooding can be configured using the **router isis lsp-fast-flooding** command. The LSP transmission can be further customized with arguments such as **max-lsp-tx**, **psnp-interval**, and **per-interface** within the samerouter isis command, and enhanced by using the **isis remote-psnp-delay** command. This feature is disabled by default, and requires manual configuration to enable.
Enhancement to the show reload-history Command	From Cisco IOS XE 17.14.1a, the **show reload-history** command is modified to **show reload history**. The output for the command is updated to include crash data, Cisco High Availability (HA) status, and software version.

Feature	Description
IP Endpoint Delay Measurement and Liveness Monitoring	This feature enables you to measure the end-to-end delay and monitor liveness towards either a specified IPv4 or IPv6 endpoint. From Cisco IOS XE 17.14.1a, you can be configure this feature using the **performance-measurement endpoint** and **performance-measurement delay-profile endpoint** commands.

Table 3: Programmability Features

Feature	Description
gNMI: Stream Subscriptions with On-Change Mode	gNMI telemetry supports on-change subscriptions on the same set of models as other telemetry protocols.
gNMI - SubscribeResponse with sync_response	The sync_response is a boolean field that is part of the SubscribeResponse response message. The sync_response message is sent after the first update message.

Table 4: Cisco Unified Border Element (CUBE) and SRST Features

Feature	Description
CUBE: Secure SIP with TLS 1.3 support	From Cisco IOS XE 17.14.1a onwards, security of the communication between the client and the server is enhanced with the support of Transport Layer Security (TLS) version 1.3 and associated cipher suites.
SRST: Secure SIP with TLS 1.3 support	Starting from Cisco Unified SRST 14.4 release, the SRST security feature is enhanced to support TLS version 1.3 and associated ciphers.

Table 5: Licensing Features

Feature	Description
500 Mbps Aggregate for Tier 1 and 250 Mbps Throughput Configuration in Autonomous Mode	Starting with this release, when you configure a throughput of 250 Mbps or T1, *if* an HSECK9 license is available on the device, then throughput is capped at 500 Mbps (transmitted or Tx data only). In earlier releases, throughput was capped at 200 Mbps Tx.

Resolved and Open Bugs - Cisco IOS XE 17.14.x

Resolved Bugs - Cisco IOS XE 17.14.1a

Identifier	Headline
CSCwi49846	FMTD crashes when SIG GRE tunnels configs are removed
CSCwi55725	SDR CLI config group issue
CSCwi61369	Device unexpectedly reloads due to SIGABRT
CSCwi35716	AAR backup preferred color is not working as expected
CSCwi53306	Unknown appID in ZBFW HSL log
CSCwf84567	Unexpected reload after re-connecting to vsmart
CSCwi14178	Failed to connect to device : x.x.x.x Port: 830 user : vmanage-admin error : Connection failed
CSCwj25493	Device crashes twice with *Critical process linux_iosd_image fault on rp_0_0* error
CSCwi40603	Memory leak in the Crypto IKMP process
CSCwf08658	Devices will flap the BFD sessions if we are in a non equilibrium state and have symmetric NAT
CSCwi35177	Device crash caused by continuous interface flap; interface associated to many ipsec interfaces
CSCwi60266	Device with enterprise certificates not forming control connections with controllers after upgrade
CSCwi67983	Tracker state log is missing when DNS Query fails
CSCwi53951	Packets with Unicast MAC get dropped on a Port Channel L2 Sub-intf after a router reboot
CSCwb25507	Add vendor specific parameter for NBAR protocol pack version
CSCwi53549	Device crashes with reason *Critical process fman_fp_image fault on fp_0_0 (rc=134)*
CSCwi82548	Crash in IKEv2 Cluster Load Balancer
CSCwi51381	TrapOID of ciscoSdwanBfdStateChange is different from MIB file
CSCwi85293	IKEv2 IPv6 Cluster Load balance: Secondary in cluster unable to connect to cluster in case of FVRF
CSCwi86698	No error message is seen while using multicast address as system-IP in SD-routing device.

Identifier	Headline
CSCwj06622	Segmentation fault and core files are seen on IOS-XE in controller-manged devices due to speedtest
CSCwi16111	IPv6 TCP adjust-mss does not work after delete and reconfigure
CSCwi62230	SIG tunnel: 'SIG STATEâ is showing blank value
CSCwj27545	Device crashes due to FTMD
CSCwj70773	Unable to create a portchannel interface with maximum number limit

Open Bugs - Cisco IOS XE 17.14.1a

Identifier	Headline
CSCwh91039	High System CPU load reported due to unsupported number of vCPUs allocated
CSCwj48393	ISG: Service with no priority is not working as expected
CSCwj48421	After onboarding device on IOTOD, OD was not able to connect with the device
CSCwj09284	Unexpected reboot in WLC due to SSL
CSCwj40589	Endpoint tracker using DNS does not log the DOWN message when the DNS server reachability is lost
CSCwj26085	[SIT]: control connections in TLS with mode; vsmart & vmanage goes to 'trying' state with UTD
CSCwj29381	Service-policy will not be applied to a new Tunnel interface when sourced using sub-interface
CSCwj45177	A *dmidecode: command not found* error is seen when executing the **show sdwan certificate validity** command
CSCwj34578	NAT46 translations are dropped when router is configured with NAT64 and as a Carrier Supporting Carrier CE
CSCwi91887	IPsec PWK SPI mismatch causes cEdge bfd tunnels to remain in down state
CSCwi81026	SDWAN BFD Sessions flapping during IPSec Rekey in scaled environment
CSCwi59854	The **show sdwan policy service-path** command gives inconsistent results when app name is specified
CSCwj02661	UTD signature update fails and device does not record the update
CSCwj43905	Unexpected reboot due to QFP-Ucode-Radium failure
CSCwj38804	ZBFW FQDN patterns missing from QFP patten-list
CSCwj02628	Speed-test does not work for cEdge device

Identifier	Headline
CSCwj30334	CVLA ucode crashes when attempting merge on used block
CSCwj49941	dns-snoop-agent has TCAM entry with all zeros for some regex patterns
CSCwi77159	Some of the objects of CISCO-SDWAN-APP-ROUTE-MIB are not implemented
CSCwj40223	appRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns wrong order
CSCwj30909	SD-Routing: Device upgrade fails with dirty config while device is in vManage mode
CSCwj27108	SD-WAN does not balance traffic to default route
CSCwj44843	Deploy of Policy Group fails after detachment of Embedded Security Policy
CSCwj31354	Template push fails due to service timestamps
CSCwj32347	DIA Endpoint tracker not working with ECMP routes when loopback is used as source

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 results 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.