Release Notes for Cisco Catalyst 8000V Edge Software, Release 26.1.x

Cisco Catalyst 8000V Edge Software, Release 26.1.x

Cisco 26.1 is the first release for Cisco Catalyst 8000V in the Cisco IOS XE 26.1.x release series.

New software features

This section provides a brief description of the new software features introduced in this release.

Table 1. New software features for Cisco Catalyst 8000V, Release 26.1

Product impact	Feature	Description
Ease of set up	Support for Microsoft HyperV on Azure Local certified servers	Cisco IOS XE 26.1.1 supports the deployment of Cisco Catalyst 8000V virtual router on Microsoft HyperV hypervisor in Microsoft HCI OS version 23H2 operating system software that runs on Microsoft Azure Local (formerly also known as Azure Stack HCI) certified servers. The deployment support includes network connectivity via NetVSC driver. Use the Cisco Catalyst 8000V .iso image and Microsoft HCI OS PowerShell CLIs for these deployments. Support for deployment on Azure Local is also enabled for Cisco Catalyst 8000V running Cisco IOS XE 17.15.5 and 17.18.2 releases. For more information, see Azure Local.
Ease of set up	Support for Nutanix AHV Hypervisor	Cisco IOS XE 26.1.1 supports the on-premises deployment of Cisco Catalyst 8000V virtual router on Nutanix AHV (Acropolis Hypervisor) bundled in Nutanix AOS version 7.3 (Acropolis Operating System). Nutanix AHV is a type-1 bare-metal hypervisor based on Linux KVM technology. Support includes SR-IOV fast-path connectivity for Nvidia Mellanox ConnectX-6 NICs. For other NICs you can use VirtIO connectivity. Use the Cisco Catalyst 8000V .iso image or the .qcow2 image for these deployments. You can perform the deployment by using Nutanix Prism Central dashboard, Nutanix Prism Element dashboard, Nutanix AOS REST APIs, or Nutanix AOS CLIs. Support for deployment on Nutanix AHV is also enabled for Cisco Catalyst 8000V running Cisco IOS XE 17.15.5 and 17.18.2 releases. For more information, see Nutanix support. For more information, see Nutanix support.
Ease of use	Support for Interface speed setting of 100 Gbps	From Cisco IOS XE 26.1.1, you can set an interface speed of up to 100 Gbps in Cisco Catalyst 8000V through command line interface. This enables some traffic profiles to see higher throughputs.
Upgrade	Support for SLES 15 SP7	Cisco IOS XE 26.1.1 supports the deployment of Cisco Catalyst 8000V on SUSE Linux® Enterprise Server (SLES) 15 SP7 operating system with KVM hypervisor.
Ease of use	Support for Nvidia Mellanox ConnectX-7 network interface cards	From Cisco IOS XE 26.1.1 release, Cisco Catalyst 8000V supports SR-IOV connectivity for Nvidia Mellanox ConnectX-7 Network Interface Cards (NICs) that deliver higher throughput and performance for the supported hypervisors.
Software reliability	DNS Security and increase the support for Local domain bypass scale to 256	From this release, the scale for Fully Qualified Domain Name (FQDN) bypass entries has been increased to 256. This allows administrators to configure up to 256 FQDNs for local domain bypass, providing greater flexibility and control over domain-specific routing and access policies within Cisco Secure Access.

Product impact	Feature	Description
Software reliability	Enhancements for NGFW in Policy Groups	This feature introduces support for NGFW Policy Groups, that includes import and export of firewall policies, display of rule hit counts, drag-and-drop rule reordering to update priority, visibility of policy and object usage references in the NGFW Dashboard, and retention of rule and policy names in the running CLI configuration.
Ease of use	One minute granularity interface statistics using Cisco Catalyst SD-WAN Manager	This feature enables the collection of granular interface statistics from devices every minute, providing real-time insights for effective troubleshooting and ensuring optimal performance.
Ease of use	BGP Advertisement Startup Delay	When a Border Gateway Protocol (BGP) process initializes during a router reload or when BGP routing sessions are reset by using the clear ip bgp* command, it could result in a temporary period of traffic loss. The BGP Advertisement Startup Delay feature addresses this issue by introducing a configurable delay before BGP begins advertising routes to its neighbors. This delay allows sufficient time for routes to be installed in the hardware, ensuring traffic forwarding is ready before new routes are announced.
Software reliability	Resilient Infrastructure	As part of the ongoing commitment to network security, this release introduces secure alternatives to legacy commands. These updates are designed to mitigate potential risks and assist in establishing a more robust and secure operational baseline. The identified insecure commands are categorized as: • Line transport: Updates to secure remote access methods. • Device server configuration: Hardening of server-side settings. • File transfer protocols: Transitioning to encrypted transfer methods. • SNMP: Enhancements to secure management traffic. • Passwords: Strengthening authentication and credential management. • Miscellaneous: General security improvements for various system functions. For all detected insecure configurations during device boot or upgrade, error messages are displayed. In Cisco IOS XE 26.1.1 release, all insecure CLI commands are blocked by default to strengthen your network infrastructure. If your environment requires the use of a legacy command, you must enable the system mode insecure command in global configuration mode. • Recommendation: Do not use insecure mode. This mode is temporary and will be removed in a future release. Identify and replace all insecure commands with their secure alternatives. • Upgrade behavior: If you upgrade to Cisco IOS XE 26.1.1 release with insecure commands already present in the running configuration, the system mode insecure command is automatically added to your configuration to prevent service disruption. For more information, refer this document Routing-SD-WAN Resilient Infrastructure
CUBE Features		

Product impact	Feature	Description
Upgrade	Advanced TLS security compliance and control	From Cisco IOS XE 26.1.1 onwards, weaker TLS versions (v1.0, v 1.1) and associated ciphers are not supported in default configurations. However, these insecure configurations are supported in "insecure operation-mode" for CUBE and SRST, and support for non-compliant ciphers has been discontinued in both platforms.
Upgrade	Dual certificate support for SIP trunk client and server functionality	From Cisco IOS XE 26.1.1 onwards, the feature allows provisioning and assigning separate certificates for client and server roles on each SIP trunk in CUBE.

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com.

Resolved issues in Cisco IOS XE 26.1

Table 2. Resolved issues for Cisco Catalyst 8000V, Release 26.1

Bug ID	Description
CSCws40263	uCode crash occurs due to Stuck Thread during NAT session DB walk
CSCwr30573	TLOC extension unable to program due to module boot up timing
CSCws89172	When start NWPI trace on muliti-VRFs and send traffic, the device crashes
CSCwr11064	Speed test session Timeout is not clear enough to get details
CSCwq77458	FMAN crash is seen after FNF configuration changes
CSCwr00088	Add CLI to change per MPLS label CEF statistics query interval on FMAN FP
CSCwr06399	Certificate verify fails and ID cert not installed after reload of device, of certs with EC Key 521
CSCwr08462	NAT router does not respond to ARP requests
CSCws62501	IOSd crash seen when "match authen-status unauthenticated" is configured
CSCwr44921	Device may reload unexpectedly with reload reason: CPU Usage due to Memory Pressure exceeds threshold
CSCwq98154	Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel
CSCwq43883	Converting L2 routed port channel to L3 is broken

Open issues

This table lists the open issues in this specific software release.

Note: This software release may contain open bugs first identified in other releases. To see additional information, click the bug ID to access the Cisco Bug Search Tool. To search for a documented Cisco product issue, type in the browser: <bug_number> site:cisco.com.

Open issues in Cisco IOS XE 26.1

Table 3. Open issues for Cisco Catalyst 8000V, Release 26.1

Bug ID	Description
CSCwr60310	SDWAN Template push or CLI config update fails due to the duplication of VTY or Async lines in the configuration
CSCwt22006	Web UI bootstrapping failure due to invalid configuration causes persistent config merge errors despite subsequent corrections
CSCwt22873	When the ip nat translation max-entries all-host 2048 command is configured, hosts attempting to open more than 2048 NAT translation entries receive an error message
CSCws66553	FPMD crash seen with with longer soak and clear sdwan omp events
CSCwt07572	Radius packet silently consumed by UTD
CSCws35252	Device loses interface IP Configuration due to corruption in NVRAM
CSCwq59240	C8000V: Gigabitethernet1 interface does not get the IP from DHCP intermittently
CSCwt28048	Preferred-color-group restrict is not honored in data policy
CSCws99246	For TCP traffic originating from the outside side of NAT, the device does not send RST packets
CSCwt29648	BadIpChecksum drops when Segment-routing MPLS is configured over IPSEC/GRE over VDSL interface
CSCwt18839	Device may reload unexpectedly with a last reload reason of " Critical process cpp_cp_svr fault" while trying to dump FIA trace outputs with the **show platform packet-trace packet all** command
CSCws95387	PCG configuration is not deleted from FP
CSCwr76176	BFD SD-WAN PMTUD: PMTU converges unexpectedly to 970 Bytes after a dbg2:1 Event
CSCws98086	When BFD sessions are created for the first time, the state starts with " Down" and the reason for state change is described as " MAX"
CSCwq00263	IPv6 IPsec packets dropped in SVTI AH in transport mode; ping fails with specific size packets

Related resources

- 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
- Configure Licenses and Throughput for Cisco Catalyst 8000V Edge Software

Legal information