Release Notes for Cisco 8000 Series Secure Routers, Release 26.2.x

© 2025 Cisco and/or its affiliates. All rights reserved.

Contents

Cisco 8000 Series Secure Routers, Release 26.2.x 3
New software features 3
New hardware features 5
Changes in behavior 6
Resolved issues 7
Open issues 11
Compatibility 12
Related resources 14
Legal information 14

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco 8000 Series Secure Routers, Release 26.2.x

Cisco IOS XE 26.2.1 is the first release for the Cisco 8000 Series Secure Routers in the Cisco IOS XE 26.2.x release series.

The Cisco® 8000 Series Secure Routers deliver the industry's most complete secure networking experience, combining cutting-edge security, routing, assurance, and SD-WAN capabilities in a unified platform. The Cisco 8000 Series is the foundation for resilient networks that scale with your business needs.

New software features

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

New software features for Cisco IOS XE 26.2.1

Table 1. New software features for Cisco 8000 Series Secure Routers, Release 26.2.1

Product impact	Feature	Description	Supported platforms
Hardware reliability	Resilient Infrastructure Changes	As part of Cisco's Resilient Infrastructure program and Cisco's commitment to secure infrastructure, this release includes additional changes aimed towards continuing to make Cisco IOS XE more secure by default. Note that some of these changes may require operational changes if you are not following secure best practices. This release includes the following changes: The RADIUS client appends the Message-Authenticator attribute (Attribute 80 HMAC-MD5) to all outgoing Access-Request packets to mitigate cryptographic forgery and Blast-RADIUS vulnerabilities (CVE-2024-3596). The RADIUS client drops incoming Access-Accept, Access-Reject, and Access-Challenge packets if the Message-Authenticator packet is absent or invalid. Ensure AAA servers (example, Cisco ISE) are configured to return Attribute 80. Outbound SSH connections enforce Trust-On-First-Use (TOFU). The device prompts to verify and store remote server host keys in the known-hosts database on first connection and validates against them on subsequent sessions. Proxy ARP is disabled by default across all routed interfaces, SVIs, and subinterfaces to reduce Layer 2 broadcast domains and prevent ARP spoofing. Configure the ip proxy-arp command explicitly if required. The embedded web server daemon is disabled by default on factory configurations to restrict unauthenticated management access. Web UI and RESTCONF require explicit enablement of the ip http secure-server command. The IOS XE device rejects unauthenticated NTP	Cisco 8000 Series Secure Routers

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description	Supported platforms
		Mode 6 and Mode 7 control queries (monlist) to prevent NTP reflection and amplification DDoS attacks. Standard time synchronization (Modes 3 and 4) is unaffected. Warning messages are emitted on the console and logged to syslog whenever legacy insecure protocols (telnet, ftp, tftp, http) are enabled in the configuration. Real-time tracking of active insecure services is published to the operational database (operDB) and YANG data models, allowing management controllers (such as Cisco Catalyst Center) to monitor security compliance. For more information, refer Resilient Infrastructure.	
Upgrade	Secure Router NGFW	Secure Router NGFW introduces Cisco Catalyst NGFW, a new security-application container for supported Cisco Catalyst 8000 Series Secure Routers. In Cisco IOS XE Catalyst SD-WAN Release 26.2.1 and Cisco Catalyst SD-WAN Manager Release 26.2.1, the feature provides workflows to install Catalyst NGFW and migrate supported settings from NGFW V1 Engine (UTD) to NGFW V2 Engine (Catalyst NGFW). IPS and IDS retain their core detection and prevention behavior while using Talos Lightweight Security Package (LSP) content. The release also adds Encrypted Visibility Engine (EVE) for encrypted-flow analysis without payload decryption and introduces Snort ML inspection for supported threats. Catalyst NGFW replaces the UTD community/subscriber signature-package workflow with independently managed LSP and Vulnerability Database (VDB) packages. LSP contains Talos rules and detectors; VDB provides application, fingerprint, and enrichment information.	Cisco 8000 Series Secure Routers
API experience	IPv6 day-0 onboarding with DHCPv6 prefix delegation	Adds DHCPv6-PD as an IPv6 address-discovery option in the ZTP/PnP workflow for Cisco IOS XE Catalyst SD-WAN devices. ZTP runs IPv4 and IPv6 address discovery in parallel, and IPv6 discovery can use stateful DHCPv6, SLAAC, or DHCPv6-PD.	Cisco 8000 Series Secure Routers
Ease of setup	EVPN VPWS over SRv6	This feature adds support for EVPN VPWS over SRv6 transport. EVPN VPWS uses EVPN signalling and SRv6 encapsulation to provide point-to-point Layer 2 VPN service between provider edge devices.	Cisco 8000 Series Secure Routers
Ease of use	Port settings for speed, duplex, and auto-negotiation	Configure speed, duplex, and negotiation auto in a single command.	Cisco 8000 Series Secure Routers

© 2025 Cisco and/or its affiliates. All rights reserved.

Product impact	Feature	Description	Supported platforms
Ease of use	Discontiguous Subnet Mask Support for IPv4 Network Object Groups	Adds support for discontiguous subnet mask entries in IPv4 data prefixes and IPv4 network object groups used by NGFW Policy. You can use discontiguous subnet mask entries in IPv4 source and destination match conditions, rule sets, object groups, and deploy-time data prefix variables.	Cisco 8000 Series Secure Routers
Ease of use	IPv6 Multicast Service Reflection	IPv6 Multicast Service Reflection enables multicast traffic translation between IPv4 and IPv6 address families, helping connect multicast networks across logical boundaries. It supports IPv6-to-IPv6, IPv4-to-IPv6, and IPv6-to-IPv4 translation on supported Cisco IOS-XE platforms.	Cisco 8000 Series Secure Routers
CUBE features			
Hardware Reliability	Support for UC applications on secure routers	Starting with Cisco IOS XE 26.2.1, CUBE and SRST applications are supported on secure routers.	C8375-E-G2, C8235-E-G2, C8235-G2, C8231-G2, C8231-E-G2, and C8355-G2
Security	Automatic conversion of password formats into secure types	Starting with Cisco IOS XE 26.2.1, it is recommended to use Type 6 (AES) for provisioning all credentials to comply with security standards. CUBE supports auto-conversion of Type 0 or Type 7 to reversible Type 6 encryption.	C8375-E-G2, C8235-E-G2, C8235-G2, C8231-G2, C8231-E-G2, and C8355-G2
Security	Security warnings for non-secure protocols	Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used. For CUBE, use secure alternatives such as HTTPS, SFTP, or SCP.	C8375-E-G2, C8235-E-G2, C8235-G2, C8231-G2, C8231-E-G2, and C8355-G2

New hardware features

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

New hardware features for Cisco IOS XE 26.2.1

Table 2. New hardware features for Cisco 8000 Series Secure Routers, Release 26.2.1

Feature	Description
Voice module support	From Cisco IOS XE 26.2.1, these voice modules are supported on Cisco 8231-E-G2, 8235-E-G2, and 8375-E-G2 platforms: • NIM-2BRI-NT/TE • NIM-4BRI-NT/TE • NIM-4E/M Support is for devices operating in Autonomous mode, not in Controller mode.

© 2025 Cisco and/or its affiliates. All rights reserved.

Feature	Description
	For information about voice module support added in release Cisco IOS XE 26.1.1, refer to the new hardware features section of the [Release Notes for Catalyst 8200 and Catalyst 8300 Release Notes, 26.1.x]

Changes in behavior

This section provides a brief description of the behavior changes introduced in this release.

Changes in behavior in Cisco IOS XE 26.2.1

Table 3. Behavior changes for Cisco 8000 Series Secure Routers, Release 26.2.1

Description	Behavior changes
The ip nat translation nonpat-timeout keyword allows configuring a timeout from 0 to 536870 seconds or setting it to never.	Refer to the ip nat translation (timeout) command.
You can verify the FEC type from the show interface command only for 100G interfaces.	Refer to the Configuring FEC section.
DHCP relay is always enabled by Cisco IOS and provide status verification for cellular modems	Refer to the Configuring the DHCP Client section.
Certificate hexadecimal data appears under crypto pki certificate chain in show running-config by default. Starting with Cisco IOS XE Release 26.2, configure the crypto pki certificate hidehex command hides certificate hexadecimal data from show running-config output while retaining the certificate chain and entry.	Refer to the Certificate Hexadecimal Data Output Example.
The procedure for configuring a trustpoint for EST is updated.	Refer to the Configure a trustpoint for EST section.
In IOS XE 26.2.1, the IOx persistent disk allocation for supported Cisco Service Routers increases from 4GB to 6GB. IOx uses part of bootflash: as persistent storage for app-hosting applications and application data, including UTD, TE, and VDSP. If the device is later downgraded from IOS XE 26.2.1 or later to an earlier release while the IOx persistent disk is 6GB, the earlier image removes the 6GB disk, creates a new 4GB disk, and applications and data stored on the IOx persistent disk are lost.	The behavior change is applicable to these platforms: • C8231-G2 • C8235-G2 • C8231-E-G2 • C8235-E-G2 • C8355-G2
DHCPv6-PD Day-0 onboarding includes vendor information for device identification.	For DHCPv6-PD Day-0 onboarding, use these commands: ▪ ipv6 dhcp client vendor-class mac-address — supplies the device MAC address in DHCPv6 Option 16. ▪ ipv6 dhcp client request vendor — requests vendor-specific information in DHCPv6 Option 17. Refer to IPv6 day-0 onboarding with DHCPv6 prefix delegation.

© 2025 Cisco and/or its affiliates. All rights reserved.

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.

Resolved issues in Cisco IOS XE 26.2.1

Table 4. Resolved issues for Cisco 8000 Series Secure Routers, Release 26.2.1

Bug ID	Description
CSCws66553	fpmd crash seen with 17.12.6B respin image with longer soak + clear sdwan omp events
CSCwt10887	SDWAN edge router device crashed after attempting to push a config group
CSCwt26644	On 26.1 vdaemon crash observed on C8000v, while forming control connetions
CSCwt39273	Config update via CLI template is failing post reboot with C8200L-1N-4T
CSCwt44263	VPN ID is not maintained after UTD feature causing ZBFW to evaluate against incorrect policy
CSCwt45748	Crash while processing packet in AppNav Tunnel
CSCwt56693	L2TP: Seeing " protocol l2tpv2 L2TP_CLASS_011" config getting lost with clear ppp all cli
CSCwt70932	BFD session establishment failed due to ARP resolution failure.
CSCwt84502	Critical Process cpp_ha_top_level_server crash (rc=69) Crash after adding zone based firewall setup configuration on the router
CSCwt87616	OTP and PSK related changes on the device
CSCwt92911	Crash in OMP process during end point tracker teardown
CSCwt94337	cpp_cp_svr crashes with SIGSEGV whle printing packet trace data
CSCwu03372	Unexpected reload due to ftmd fault on SDWAN edge router with On-Demand Tunnels
CSCwu27070	Unexpected Reload in CPP Server (cpp_sp_svr) Code
CSCwu30605	17.18 SIG ipsec primary tunnel going down after source interface change
CSCwu35982	Router unexpectedly reloads after IKEv2 operations
CSCwu39202	SDWAN edge router : Power reset during cEdge boot causes router to enter ROMMON
CSCwu47545	Ucode Code Crash while Printing Log for FW Drop for Packet with Invalid Header
CSCwu49029	Unexpected reload on CGM (Class-Group Manager) when updated
CSCwu51162	Unexpected reload on router in SDWAN CCE (Classifier and Classification Engine)

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwu61766	SDWAN edge router OMPD crash on malformed SD-WAN identity IP-to-user update from vSmart pxGrid integration
CSCwu67470	Unexpected reload on SDWAN edge router device after changing secuity policy to none on template
CSCwu86821	Service-chain config modify to local svc-chain failed to delete old TLOC list action leading to packet drops
CSCwv25887	High QFP utilization due to NAT translation timeout and concurrent translation creation causing allocator contention
CSCwv60786	Intermittent issue with RRI being lost on the Flex Hub
CSCwv71880	SD-WAN redirect-dns Destination NAT session collides with SIG tunnel IKEv2 control plane traffic
CSCwv96043	Pkt Dup fails in SymNAT scenario with aggressive BFD timers
CSCww00071	Router crashed while decrypting NAT-T IPsec traffic with CTS SGT enabled
CSCww15035	C8375-E-G2: IOS XE 26.1/26.2 UTD hits high QFP utilization and sustained MemoryInterfaceDrop near 700-742 Mbps, regression from 3.2 Gbps on 17.18.x
CSCwr02102	Router intermittently loses ip address dynamically assigned to tunnel interface
CSCwr49368	SSE Tunnels with Cisco Secure Access are stuck in SD-WAN Configuration Database
CSCwr60310	SDWAN Template push or CLI config update fails due to the duplication of VTY or Async lines in the configuration
CSCwr76176	BFD SD-WAN PMTUD: PMTU Converges Unexpectedly to 970 Bytes After dbg2:1 Event
CSCws50867	17.18/26.1: Tracker probe id set to 0 while changing Invalid DNS endpoint to endpoint-ip
CSCws68686	Application Policy: IPv6 BGP Neighborship Fails When Using Basic Policy with Default Drop Action
CSCws95879	ICMP TTL Expired packet sent via incorrect VRF
CSCws98086	Update " reason for state change: MAX" in BFD Syslog
CSCwt16689	QFP command displays incorrect App-Probe-Class (APC) queue assignment
CSCwt17412	Sessions appear as two unidirectional records instead of one bidirectional flow
CSCwt25903	Not able to disable " log" feature in NGFW Policies vManage for " Drop" rules.
CSCwt46462	Enable alerts for the EC genet server (Transform) dying or timing out
CSCwt47734	Endpoint-tracker HTTP probe sends IP address instead of FQDN in 17.15
CSCwt66413	ncsshd process fails to terminate after " no netconf" and netconf refuses connection

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwt67685	SD-WAN Edge: Periodic Service Restart May Generate Crash Files
CSCwt75037	Device in controller mode crashes with Critical process cpp_ha_top_level_server fault on fp_0_0 (rc=69)
CSCwt79827	IOS-XE not parsing transform payload with unknown attributes
CSCwt97049	Buffer Overflow in Domain Name Pattern Handling Causes Pointer Corruption and System Crash
CSCwu03035	SDWAN edge router: UTD may silently drop large fragmented RADIUS packets
CSCwu10100	Endpoint tracker is unable to determine next-hop for DNS name resolution from Dialer interface
CSCwu21490	Kernel Core Files Deleted From Flash When Incomplete Admin Tech is Generated
CSCwu31509	Secondary OU is not generated in CSR for SD-Routing(Autonomous mode) devices
CSCwu49303	Memory Leak in cpp_sp_svr due to Classification Objects
CSCwu53168	SDWAN edge router upgrade fails with " timeout" when confd Phase 0 failure
CSCwu53407	Standalone endpoint-tracker UP recovery syslog missing intermittently on SDWAN edge router
CSCwu76495	SDWAN: Crash while updating Adaptive QOS Session Policy due to minimal traffic size
CSCwu83262	L2TPv3 xconnect session fails to establish when the traffic traverses through IPsec tunnel interface.
CSCwv02835	[IOS XE] 6VPE: Locally terminated IPv6 traffic fails over BDI interface
CSCwv02836	SDWAN edge router: upgrade process may report enormous " Required space"
CSCwv08826	SDWAN edge router : BOW in EAAR not working when tunnels are outside SLA and outside variance
CSCwv09160	HTTP SIG Tracker trying to resolve endpoint-api-url IP address via DNS after upgrade to 17.15.05
CSCwv23165	BFD echo packet counters report a fixed 2:1 tx/rx ratio (false 50% packet loss) on all tunnels after enabling Enhanced Application Aware Routing
CSCwv34598	SDWAN edge router Router Reset due to PuntInject Keepalive Timeout (No Ucode File Generated)
CSCwv42272	NULL Dereference in NHRP MIB
CSCwv52757	UDP packets multicast destination not seen on FIA-Trace nor EPC over xconnect
CSCwv61185	C8000V vdaemon may flap SD-WAN control connections with HWCERTREN when multiple vManage-signed edge certificates have identical Not Before timestamps.
CSCwv67035	Ikev2 PPK Unable To Switch Back to PSK When 'Required' Is Used in Keyring

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCwv73701	Packet reordering observed when application performance-monitor service policy enabled
CSCwe19394	C8200-G2: device may boot up into prev_packages.conf due to power outage
CSCwq77322	C8500-12X sending a 2 Byte packet of FLOW_SAMPLER_RANDOM_INTERVAL instead of a 4-Byte packet
CSCwq98154	C8200-G2: Multicast traffic not forwarded over P2P DMVPN phase 1 tunnel
CSCwq98206	C8200-G2:EPBR set interface action get missing after reboot
CSCwr24031	C8200-G2: After upgrade to 17.15 for earlier releases sd-wan service-tracker in vrf selects source IP address from GRT when MPLS Inter-AS VPN option B configured
CSCwr49475	C8200-G2: BFD sessions flapping and not recovering - SYMNAT port not updating to data-plane
CSCwr64257	C8200-G2: Unexpected reload on ftmd SDWAN device
CSCwr72709	C8200-G2:Router crash in TDM-TDM call when debug voip fpi enabled
CSCwr77958	C8200-G2: NWPI not capturing self-generated syslog traffic
CSCwr95551	c8kv crashes when configuring SSL VPN with Policy-Based Routing (PBR) and NAT
CSCws33781	C8200-G2: Device May Unexpectedly Reload When HA Path Optimization Is Enabled
CSCws43190	C8200-G2:Router randomly terminating an incoming PPP session on either a Virtual-Access interface or a Dialer / physical interface
CSCws66679	C8200-G2: Crash while sending stress large packet size traffic
CSCwt25835	C8455-G2: router crashed during ipsec scale periodic rekey
CSCwt42365	C8200-G2 and C8300-G2 - 0/0 remained stuck in the booting state during the reload stress test
CSCwt62618	C8100-G2 series not processing unexpected/unrecognized IPv6 Next Header correctly
CSCwu93056	Device may reload after remove an endpoint.
CSCww15597	C8130-G2 : Unexpected reload when LAN Switch is connected.
CSCwu02842	Unexpected reload due to race condition in QoS service group configuration.
CSCwu34418	QFP crash with qfp-ucode and cpp_cp_svr cores.
CSCwv99001	ipv6 dhcp client request vendor' command missing in day-0 ZTP DHCPv6 PD configs
CSCwv67341	ipv6 dhcp client vendor-class mac-address' command missing in day-0 ZTP DHCPv6 PD configs

© 2025 Cisco and/or its affiliates. All rights reserved.

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.

Open issues in Cisco IOS XE 26.2.1

Table 5. Open issues for Cisco 8000 Series Secure Routers, Release 26.2.1

Bug ID	Description
CSCwv71872	CoR-SaaS custom-app endpoint-url probing on free configurable port
CSCwv80846	IOSd crash in router_init due to stale PDB pname during routing process creation
CSCwv84068	17.12.6 likely change in the SDWAN edge router code is causing the control connections failing to come up
CSCwv86632	IOSd crash in " Open DNS Dev-Reg" process on 17.12.6 despite CSCwp09231 fix (Umbrella device-registration UAF during config churn)
CSCwv91595	Secondary IP Address not working in a Cat8200L as it was in an ISR1900 router.
CSCwv91764	CSCwv91764 - 26.2 Zscaler SSE GRE:The Public IP address for every tunnels entered on the vManage doe
CSCwv92282	SDWAN Degradation of ~6% seen in profiles IPSEC_MCAST-512V_1400 and IPSEC_QOS_DPI_FNF_MCAST-512V_1400
CSCwv92753	SDWAN: Performance Degradation seen with UTD Snort 3.12.x.0 version
CSCwv98085	SDWAN 17.18.2- Cli config push fails, SDWAN edge router displays Error: application communication failure> while running " show sdwan running"
CSCww00540	SDWAN edge router - 17.12.8 endpoint-tracker reports all shared-tracker tunnels Down when one tunnel fails DNS
CSCww11239	When hub primary tunnel goes down, few packets are lost with bfd time aggressive
CSCww14946	26.1.2: Pkt Dup does silent drop when BFD goes down with SymNAT in the mix
CSCww17900	V-Fail CSCwv95282: NGFW container Resource Profile change from low to medium fail
CSCww25858	SIG tracker routes not withdrawn on DNS re-resolution failure due to PROBE_STATE_LIVE gate — traffic blackhole (17.15+ regression)
CSCwu24210	SDWAN edge router .sdwaninstaller accounting for rollback files in disk space calculation
CSCwv61920	Standby RP Rebooting Frequently After Applying Static Named NAT Entry
CSCwv65418	SDWAN ICMP interface tracker goes up everytime the router resolves the DNS-name configured
CSCww00586	UTD context with no inspection features enabled stays in Divert mode; traffic black-holed at memif

© 2025 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description
CSCww02502	Umbrella tunnels down, reporting cdb-validate-info failed state with 401 authentication error.
CSCww05599	Unexpected reload due to NAT pool exhaustion
CSCww20413	Update outdated GeoDB in 17.18.x
CSCww26726	C8211-G2: Device crashed @pmd_pkt_copy_out while GPME maps a 4790-byte packet
CSCwp97178	C8200-G2: flapping nat will casue bfd session down with ipsec session shown
CSCwq24119	C8200-G2: Traceback seen when detaching the CN railways customer configs in 17.19
CSCwr88206	C8200-G2 table routes: Next Hop (NH) ID 0 is getting corrupted and assigned to a value other than Blackhole
CSCwr30573	C8200-G2: TLOC Extension unable to program due to module boot up timing
CSCwr76176	C8200-G2: PMTU Converges Unexpectedly to 970 Bytes After dbg2:1 Event

Compatibility

ROMMON compatibility matrix for Cisco 8100, Cisco 8200 and Cisco 8300 Series Secure Routers

This table lists the ROMMON requirements for Cisco 8100, Cisco 8200 and Cisco 8300 Series Secure Routers only. There are no separate ROMMON requirements for these routers:

- Cisco 8400 Series Secure Routers
- Cisco 8500 Series Secure Routers

Table 6. Supported ROMMON release for Cisco IOS XE 26.1.x releases

Platforms	Cisco IOS XE Release	Minimum ROMMON Release supported for IOS XE	Recommended ROMMON Release supported for IOS XE
Cisco 8100 Series Secure Routers			
C8130-G2	26.2.1	17.18(1r)	26.1(2r)
C8140-G2	26.2.1	17.18(1r)	26.1(2r)
C8151-G2	26.2.1	17.18(1r)	26.1(2r)
C8161-G2	26.2.1	17.18(1r)	26.1(2r)
C8131-G2	26.2.1	26.1(4r)	26.1(4r)
C8130-VAI-G2	26.2.1	26.1(3r)	26.1(3r)
C8130-VAP-G2	26.2.1	26.1(3r)	26.1(3r)

© 2025 Cisco and/or its affiliates. All rights reserved.

Platforms	Cisco IOS XE Release	Minimum ROMMON Release supported for IOS XE	Recommended ROMMON Release supported for IOS XE
C8151-CVAI-G2	26.2.1	26.1(3r)	26.1(5r)
C8151-CVAP-G2	26.2.1	26.1(3r)	26.1(5r)
Cisco 8200 Series Secure Routers			
C8231-G2	26.2.1	17.18(1.5r).s1.cp	17.18(4.1r).s1.cp
C8235-G2	26.2.1	17.18(1.5r).s1.cp	17.18(4.1r).s1.cp
C8231-E-G2	26.2.1	17.18(1.5r).s1.cp	17.18(4.1r).s1.cp
C8235-E-G2	26.2.1	17.18(1.5r).s1.cp	17.18(4.1r).s1.cp
Cisco 8300 Series Secure Routers			
C8375-E-G2	26.2.1	17.15(3.2r).s2.cp	17.18(3r).s2.cp
C8355-G2	26.2.1	17.15(1.18r).s2.cp	17.18(3r).s2.cp

Upgrade ROMMON

To upgrade the ROMMON version of your device, use these steps:

1. Check the existing version of ROMMON by using **show rom-monitor r0** command. If you are installing Cisco IOS XE software on a new device, skip this step.
2. Review ROMMON Compatibility Matrix to identify the recommended version of ROMMON software for the device you plan to upgrade.
3. Go to https://software.cisco.com/# and download the ROMMON package file.
4. Copy the ROMMON file to flash drive:

   copy ftp://*username*:*password*@*IP address*ROMmon package file* **flash:**
5. Upgrade the ROMMON package using the following command:

   upgrade rom-monitor filename bootflash:*ROMmon package name* **all**
6. Execute **reload** command to complete the ROMMON upgrade process.
7. Execute **show rom-monitor r0** command to ensure the ROMMON software is upgraded.

Cisco SD-WAN for Cisco 8100 Series Secure Routers

Cisco SD-WAN is enabled on a few Cisco 8100 Series Secure Routers, which earlier supported only the Routing mode.

These platforms can be configured and managed by Cisco SD-WAN Manager and can work in controller-managed mode from Cisco IOS XE Release 26.2.1.

- C8130-G2

© 2025 Cisco and/or its affiliates. All rights reserved.

- C8140-G2
- C8130H-G2
- C8130-VAI-G2
- C8130-VAP-G2

NOTE: NGFW and Thousand eyes features are not supported on C8130-G2, C8140-G2, C8130H-G2, C8130-VAI-G2 and C8130-VAP-G2 routers.

Related resources

Paltform	Guides
Cisco 8100 Series Secure Routers	Hardware Installation Guide for Cisco 8100 Series Secure Routers Software Configuration Guide for Cisco 8100 Series Secure Routers
Cisco 8200 Series Secure Routers	Hardware Installation Guide for Cisco 8200 Series Secure Routers Cisco 8200 Series Secure Routers Software Configuration Guide
Cisco 8300 Series Secure Routers	Hardware Installation Guide for Cisco 8300 Series Secure Routers Software Configuration Guide for Cisco 8300 Series Secure Routers
Cisco 8400 Series Secure Routers	Hardware Installation Guide for Cisco 8400 Series Secure Routers Software Configuration Guide for Cisco 8400 Series Secure Routers
Cisco 8500 Series Secure Routers	Hardware Installation Guide for Cisco 8500 Series Secure Routers Software Installation Guide for Cisco 8500 Series Secure Routers
Licensing	Cisco 8000 Series Secure Routers Licensing

Legal information

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: www.cisco.com/go/trademarks. 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. (1110R)

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.

© 2026 Cisco Systems, Inc. All rights reserved.