Release Notes for Cisco IOS XE SD-WAN Release 16.12.x

First Published: 2019-08-15

Last Modified: 2021-03-31

Release Notes for Cisco IOS XE SD-WAN Release 16.12.x

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

These release notes accompany the Cisco IOS XE SD-WAN Release 16.12.x, which provides Cisco SD-WAN capabilities for Cisco IOS XE SD-WAN devices. They include release-specific information for Cisco vSmart Controllers, Cisco vBond Orchestrators, Cisco vManage, as applicable to Cisco IOS XE SD-WAN devices.

For release information about Cisco vEdge routers, refer to Release Notes for Cisco SD-WAN Release 19.2.x.

Supported Devices

For device compatibility information, see Cisco SD-WAN Device Compatibility.

What's New for Cisco IOS XE SD-WAN Releases 16.12.1b, 16.12.1d, and 16.12.2r

This section applies to Cisco IOS XE SD-WAN devices.

Cisco is constantly enhancing the SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides. For information on additional features and fixes that were committed to the SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

Table 1: What's New for Cisco IOS XE SD-WAN Devices

Feature	Description
Getting Started	

Feature	Description
API Cross-Site Request Forgery Prevention	This feature adds protection against Cross-Site Request Forgery (CSRF) that occurs when using Cisco SD-WAN REST APIs. This protection is provided by including a CSRF token with API requests. You can put requests on an allowed list so that they do not require protection if needed. See Cross-Site Request Forgery Prevention.
Systems and Interfaces	
IPv6 Support for NAT64 Devices	This feature supports NAT64 to facilitate communication between IPv4 and IPv6 on Cisco IOS XE SD-WAN devices. See IPv6 Support for NAT64 Devices.
Secure Shell Authentication Using RSA Keys	This feature helps configure RSA keys by securing communication between a client and a Cisco SD-WAN server. See SSH Authentication using vManage on Cisco XE SD-WAN Devices. See Configure SSH Authentication.
DHCP option support	This feature allows DHCP server options, 43 and 191 to configure vendor-specific information in client-server exchanges. See Configure DHCP.
Communication with an UCS-E Server	This feature allows you to connect a UCS-E interface with a UCS-E server through the interface feature template. See Create a UCS-E Template.
Bridging, Routing, Segmentation, and QoS	
QoS on Subinterface	This feature enables Quality of Service (QoS) policies to be applied to individual subinterfaces. See QoS on Subinterface.
Policies	
Packet Duplication for Noisy Channels	This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video. See Configure and Monitor Packet Duplication.
Control Traffic Flow Using Class of Service Values	This feature lets you control the flow of traffic into and out of a Cisco device's interface based on the conditions defined in the quality of service (QoS) map. A priority field and a layer 2 class of service (CoS) were added for configuring the re-write rule. See Configure Localized Data Policy for IPv4 Using Cisco vManage.
Integration with Cisco ACI	The Cisco SD-WAN and Cisco ACI integration functionality now supports predefined SLA cloud beds. It also supports dynamically generated mappings from a data prefix-list and includes a VPN list to an SLA class that is provided by Cisco ACI. See Integration with Cisco ACI.
Encryption of Lawful Intercept Messages	This feature encrypts lawful intercept messages between a Cisco IOS XE SD-WAN device and a media device using static tunnel information. See Encryption of Lawful Intercept Messages.

Feature	Description
Security	
High-Speed Logging for Zone-Based Firewalls	This feature allows a firewall to log records with minimum impact to packet processing. See Firewall High-Speed Logging.
Self zone policy for Zone-Based Firewalls	This feature can help define policies to impose rules on incoming and outgoing traffic. See *Apply Policy to a Zone Pair* in Use the Policy Configuration Wizard.
Secure Communication Using Pairwise IPsec Keys	This feature allows you to create and install private pairwise IPsec session keys for secure communication between an IPsec device and its peers. See IPSec Pairwise Keys Overview.
Network Optimization and High Availability	
TCP Optimization	This feature optimizes TCP data traffic by decreasing any round-trip latency and improving throughput. See TCP Optimization: Cisco XE SD-WAN Routers.
Share VNF Devices Across Service Chains	This feature lets you share Virtual Network Function (VNF) devices across service chains to improve resource utilisation and reduce resource fragmentation. See Share VNF Devices Across Service Chains.
Monitor Service Chain Health	This feature lets you configure periodic checks on the service chain data path and reports the overall status. To enable service chain health monitoring, NFVIS version 3.12.1 or later should be installed on all CSP devices in a cluster. See Monitor Service Chain Health.
Manage PNF Devices in Service Chains	This feature lets you add Physical Network Function (PNF) devices to a network, in addition to the Virtual Network function (VNF) devices. These PNF devices can be added to service chains and shared across service chains, service groups, and a cluster. Inclusion of PNF devices in the service chain can overcome the performance and scaling issues caused by using only VNF devices in a service chain. See Manage PNF Devices in Service Chains.
Devices	
Cisco 1101 Series Integrated Services Routers	Cisco SD-WAN capability can now be enabled on Cisco 1101 Series Integrated Services Routers.
Commands	
Loopback interface support for WAN (IPsec)	This feature allows you to configure a loopback transport interface on a Cisco IOS XE SD-WAN device for troubleshooting and diagnostic purposes. See the bind command.

New and Enhanced Hardware Features

New Features

- Support for UCS-E module—This feature adds a UCS-E template in Cisco vManage for configuring Cisco Unified Computing System (UCS) E-Series servers. For related information, see Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine and Configuring Devices using vManage.

Note Currently, backplane interfaces are not supported for UCS-E module. Only external connectivity is supported.

- Support for Cisco IR1101 Integrated Services Router Rugged—Cisco SD-WAN capability can now be enabled onCisco IR1101 Integrated Services Router Rugged. The following notes apply to this support:
  - Controller devices (Cisco vBond orchestrators, Cisco vManage NMSs, and Cisco vSmart controllers) must run Cisco SD-WAN Release 19.2 or later.
  - The default topology is full mesh, but the hub and spoke topology is often used for IoT applications.
  - Cisco SD-WAN support on the Cisco IR1101 Integrated Services Router Rugged requires Cisco IOS-XE Release 16.12.
  - The Cisco IR1101 Integrated Services Router Rugged has four fixed switch-ports. Make sure to select the correct template.
  - The CLI template is not currently supported.
  - Starting from Cisco IOS-XE Release 16.12.1, Cisco IR1101 Integrated Services Router Rugged has dual LTE support with LTE extension module.
  - We recommend using up to 50 BFD sessions for scaling.

Important Notes, Known Behavior, and Workaround

- Cisco IOS XE SD-WAN devices with the SFP-10G-SR module do not support online insertion and removal (OIR) of this module.
- When you complete a Cisco SD-WAN software downgrade procedure on a device, the device goes into the configuration mode that it was in when you last upgraded the Cisco SD-WAN software on the device. If the device is in a different configuration mode when you start the downgrade than it was when you last upgraded, the device and Cisco vManage show different configuration modes after the downgrade completes. To put the configuration modes back in sync, reattach the device to a device template. After you reattach the device, both the device and Cisco vManage show that the device is in the vManage configuration mode.

Cisco vManage Upgrade Paths

Table 2:

Starting Cisco vManage Version	Destination Version
	19.2.x
18.x/19.2.x	Direct Upgrade
20.1.x	Not Supported
20.3.x	Not Supported
20.4.x	Not Supported

Resolved and Open Bugs

About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

Resolved and Open Bugs

This section details all fixed and open bugs for this release. These bugs are available in the Cisco Bug Search Tool

Resolved Bugs for Cisco SD-WAN Release 16.12.5

Resolved Bugs for Cisco SD-WAN Release 16.12.5

Table 3: Resolved Bugs for Cisco SD-WAN Release 16.12.5

Bug ID	Description
CSCvn60531	real time omp advertised routes in vmanage showing received routes as well.
CSCvt42415	Traceback: cEdge unexpected reload by 'fpmd' process when vManage pushes policy change
CSCvu07639	UTD policy on global VPN does not work properly for DIA traffic
CSCvu80611	cpp_cp_svr_ledp crash seen during SIT Regression
CSCvv14263	Day 0 Config Bringup after Power OFF/ON | C1121X-8PLTEP
CSCvv27342	vManage configuration for device not seen in NCS post upgrade from 19.2.2 to 19.2.3
CSCvv43700	c1100 LTE router showing incorrect value in "sh ip route" output

Bug ID	Description
CSCvv73691	PMTU Discovery may negotiate an incorrect MTU on XE SDWAN routers
CSCvw62805	SDWAN ZBFW CPU punted traffic mishandling -- Out2In packet looped

Resolved and Open Bugs for Cisco SD-WAN Release 16.12.4

Resolved Bugs for Cisco SD-WAN Release 16.12.4

Table 4: Resolved Bugs for Cisco SD-WAN Release 16.12.4

Bug ID	Description
CSCvs35368	ISR 4331 rebooted with "CPU Usage due to Memory Pressure exceeds threshold" when running traffic
CSCvs65449	Leftover files on C1111-8LTELA While Adding Software to the Partition
CSCvs68349	16.12.3 ZBFW- Firewall stats file for vmanage not generated for inspect/drop traffic
CSCvs69535	Software upgrade from version 16.12.1e to 16.12.02r failed - auto upgrade-confirm did not happen
CSCvt02574	vmanage incorrectly deletes a physical cellular link 0/2/1 during template push
CSCvt04864	cpp_cp_svr fault and fman_fp_image fault on ASR 1002-x routers running 16.12.2r
CSCvt12245	16.12.3 ZBFW-Mismatch in firewall stats between the device and vmanage
CSCvt16595	XE SDWAN routers experience slow memory leak over time in 'ncsshd' process
CSCvt21691	VLAN1 is allowed on the trunk port even though it is not allowed in configurations of C111 interface
CSCvt35444	XE SDWAN router crashes with cFlowd enabled
CSCvt37676	Cisco IOS XE SD-WAN crashes after changing flow-sampling-interval within a cflow policy
CSCvt52168	SSH Process Thrash During Normal Operations
CSCvt57024	Cisco IOS XE SD-WAN reboot multiple times with nested back trace
CSCvt65298	VRRP issue with vEdge-5k
CSCvt98034	BGP communities: changes to route-map which sets BGP communities discards existing communities
CSCvu18773	[DyT]: Cxp doesn't compute loss/latency even with reachability due to Tracker status down
CSCvu22003	vManage FW dashboard doesn't show all matched applications
CSCvu45109	CSR: Azure AN: MLX5 driver fails to load in 16.12.2 & 16.12.3

Bug ID	Description
CSCvu70571	SDWAN router ASR1001-X crashes when object-group service configuration is added
CSCvs75505	Cisco IOS XE SD-WAN Software Command Injection Vulnerability

Open Bugs for Cisco SD-WAN Release 16.12.4

Bug ID	Description
CSCvq22687	<ip name-server vrf 1> configuration not saved upon upgrade from 16.9 to 16.10
CSCvt35353	Manually configured TCP MSS adjust does not affect datapath
CSCvt81979	ASR IOS-XE SDWAN router bfd sessions not coming up if BGP routing is not providing a local next hop.
CSCvu85370	ASR1001HX PMTU process not working all the time

Resolved and Open Bugs for Cisco SD-WAN Release 16.12.3

Resolved Bugs for Cisco SD-WAN Release 16.12.3

Table 5: Resolved Bugs for Cisco SD-WAN Release 16.12.3

Bug ID	Description
CSCvm86435	confd_cli process is not terminated and hogging CPU
CSCvp86463	key field of yang-model "snmp-server/host" incorrect
CSCvq32705	push config error on console SDWAN ERR: SDAVC :: global enable failed
CSCvq58755	isrv_XE-SDWAN : IOS startup config and confd config are out of sync
CSCvr12395	vManage push "media-type rj45" when trying to configure duplex on ISR1k
CSCvr48928	Template push stuck on vManage Cluster when pushing new System IP to Edge router
CSCvr89182	ISR4331 fails upgrade to 16.12.1d and rollsback with ASR1001-HX identity
CSCvs43170	[vManage] Firewall inspect/drop stat values are incorrect on device dashboard
CSCvs56121	sysmgrd core seen on CSR on reboot cases
CSCvs56346	template push fails for ipv6 BGP nbr on upgrade scenario from 19.2.097/098
CSCvs57742	Cisco XE SDWAN devices VRF 1 BGP to VRF 1 EIGRP redistribution not working
CSCvs61118	DHCP Lease error when we push template
CSCvs62737	SD-AVC service is disabled and cannot be enabled
CSCvs70680	IPv6 prefix lists are erased with the upgrade

Bug ID	Description
CSCvs72351	Bootstrap file "ciscosdwan.cfg" not working in controller mode
CSCvs75634	16.12.3 ZBFW:Configuration database locked by vmanage-session
CSCvs90207	On Cisco XE SD-WAN devices all the BFD session flap if there is a control connection flap to vmanage
CSCvs98389	Packet drops in XE-SDWAN because of "IN_CD_COPROC_ANTI_REPLAY_FAIL" errors
CSCvt07635	Eigrp redistr protocol with route policy is not showing in XE_SDWAN after template push fr vManage
CSCvm42581	ftmd crash while changing rewrite rule PLP from high to low
CSCvq35040	the configuration database is locked by session <id> system tcp git/vdaemon/vdaemon_misc.c
CSCvs72576	VRRP on vEdge on Hyper-V not working as expected; Both vEdges show "master"
CSCvt46779	Route export not working as desired during failover testing

Open Bugs for Cisco SD-WAN Release 16.12.3

Table 6: Open Bugs for Cisco SD-WAN Release 16.12.3

Bug ID	Description
CSCvs35368	ISR 4331 rebooted with "CPU Usage due to Memory Pressure exceeds threshold" when running traffic
CSCvs78390	TLS connection does not come up with 16.12.x, but with 16.10.x works fine
CSCvs88835	ASR1001-X periodic crash with scale BFD sessions - FTMD usage at over 5GB
CSCvs90555	Template push fails when enabling ipv4 addr family on BGP ipv4 neighbor
CSCvt02574	vmanage incorrectly deletes a physical cellular link 0/2/1 during template push
CSCvt12245	16.12.3 ZBFW-Mismatch in firewall stats between the device and vmanage
CSCvt21691	VLAN1 is allowed on the trunk port even though it is not allowed in configurations of C111 interface
CSCvt28539	explicit acl needed for cellular intf for control connection bringup
CSCvt30997	qfp_ucode crashed with unexpected reboot along with fman_fp crash
CSCvt32672	Banner login and motd messages are displayed before login for telnet console
CSCvu18315	c1121 cEdge- VLAN config inconsistent between "show run" and "show sdwan run"

Resolved and Open Bugs for Cisco SD-WAN Release 16.12.2r

Resolved Bugs for Cisco SD-WAN Release 16.12.2r

Table 7: Resolved Bugs for Cisco SD-WAN Release 16.12.2r

Bug ID	Description
CSCvp38857	unable to modify interface speed for CSRv XE SDWAN
CSCvr45260	The config on VBond rolls back when the configs are pushed through VManage CLI template
CSCvr51104	vManage cluster GUI SSO fails during the 2nd login attempt using old cookies
CSCvk32783	Standard IPSec support in IOS-XE SDWAN software
CSCvp11416	XE SD-WAN device- Template attach fails for a Cisco XE SD-WAN device if theres a central policy with cflowd activated
CSCvp36883	SD-WAN QoS not work as expected after no class under policy-map
CSCvp37056	flow-visibility get broken and doesn't working properly on ASR1001HX platform with IPSec encap
CSCvp73389	OSPF is not setting the downbit for the default route.
CSCvp96887	Failed to attach template to Cisco XE SDWAN Rtr if qos-map name changed after policy-map is attached
CSCvq01813	Pending object for "SDWAN Overlay Cfg" and sessions are not downloaded with scale of sdwan session
CSCvq27599	Delete bandwidth queue with random-detect from template getting rejected on device side
CSCvq31153	SDWAN BFD session stuck and packet drops due to IN_CD_SW_IPSEC_ANTI_REPLAY_FAIL drops
CSCvq47444	CLI "config-exchange request" for any ikev2 profile has inconsistent behavior between IOS and confd
CSCvq49150	LAN ACL dropping packets with default-action accept
CSCvq64513	Differentiate sdwan control packets priority based on device_type for Inject path
CSCvq65906	admin/admin credentials are lost after reload
CSCvq66518	Data traffic classified into qos-group 0 improperly without qos policy enabled
CSCvq68449	QFP ucode reloads unexpectedly while processing large packet with NBAR enabled
CSCvq75871	IPSec SA receives anti-replay error for all packets for NAT session flap sometimes

Bug ID	Description
CSCvq76075	HMAC failure due to incorrect stale nat fixup entry for the ipsec session after symnat session flap
CSCvq97694	Local internet breakout (DIA) doesn't work on subinterfaces in IOS-XE SD-WAN 16.11.1a, 16.12.1b
CSCvr12264	fman-fp crashed with "set vpn + tloc" in data-policy with tloc pointed to local
CSCvr23424	XE SD-WAN device rebooting continuously when upgraded to 16.12b
CSCvr23454	NBAR not turned off on datapath when unconfigure policy with app-visibility
CSCvr28506	ftpmd process core when two app-ids with invalid name used in centralized app-route-policy
CSCvr46085	QoS dscp rewrite doesn't work properly with one single rewrite-rule entry update
CSCvr47688	local data policy classification issue with prefix less specific than /24 on ISR1100 platform
CSCvr52767	loops because of redistribution OMP<>OSPF external with DN-bit are happening on IOS-XE SD-WAN
CSCvr55738	spanning-tree mode rapid-pvst is not part of the default config on 16.12.1 Cisco XE SD-WAN software anymore
CSCvs34879	Tracebacks seen when pushing ACL policy on C1111-8P
CSCvs46366	DNS configurations are not pushed to the XE-SDWAN device properly
CSCvp86463	key field of yang-model "snmp-server/host" incorrect
CSCvq45411	IOSd is crashing after configuration from vmanage is pushed
CSCvq69544	Improve datapath drop cause with proper code for OCT_UNSUPPORTED_CIPHER from Octeon based platform
CSCvr18395	policy seq with app-family network-service is not downloaded to datapath
CSCvr27773	Multiple times add and delete sym nat with Cisco XE SD-WAN device cause BFD down with vEdge devices
CSCvr27819	Add/remove of symmetric nat on WAN link multiple times makes the link BFDs down forever
CSCvr48167	SD-WAN BFD session failure due to IPSec SA is down and stuck with non IPSec SA

Open Bugs for Cisco SD-WAN Release 16.12.2r

Table 8: Open Bugs for Cisco SD-WAN Release 16.12.2r

Bug ID	Description
CSCvm86435	confd_cli process is not terminated and hogging CPU
CSCvr22877	BFD staying down between a XE SD-WAN device and a Cisco vEdge device after a failure condition is triggered on the ISP side.
CSCvs27051	idle-timeout is improperly mapped on XE SD-WAN devive
CSCvs39216	IOS-XE SD-WAN CSR in Azure does not remove start up config.
CSCvs54333	c1100-4P/6P-LTE : Low Bandwidth over cellular is not working
CSCvs56121	sysmgrd core seen on CSR on reboot cases
CSCvp86463	key field of yang-model "snmp-server/host" incorrect
CSCvs94771	19.2.1 template push failing for 16.10.2 Cisco XE SD-WAN devices

Resolved Bugs for Cisco SD-WAN Release 16.12.1e

Table 9: Resolved Bugs for Cisco SD-WAN Release 16.12.1e

Bug ID	Description
CSCvp96887	Failed to attach template to Cisco XE SDWAN Rtr if qos-map name changed after policy-map is attached
CSCvq10160	Cellular IP is getting reset when primary transport interface Gi0/0/0 is shutdown.
CSCvq11615	Route is not getting removed from the routing table even if the BFD is down.
CSCvq61835	interface cant be moved from vrf 0 to service vrf when it has ip address
CSCvq61992	XE SDWAN router stuck in boot loop after power-cycle due to replaystore file corruption
CSCvq70071	flow data is not populated into /tmp/xml/fnf
CSCvq97954	Cellular interface doesn't get an IP address when brought up through the pnp workflow
CSCvr13244	19.2.0 regression: Can not configure NTP on SD-WAN and specify source interface in VPN
CSCvr15012	fman-fp keeps on crashing after attach app-route policy with app-family
CSCvr18082	xe-sdwan omp aggregate-only does not suppress component routes sometimes
CSCvr35568	CPP crash with Packet Duplication enabled on path failover with XE SDWAN router

Bug ID	Description
CSCvr52767	microloops because of redistribution OMP<>OSPF external with DN-bit are happening on IOS-XE SD-WAN
CSCvq11615	Route is not getting removed from the routing table even if the BFD is down.
CSCvq61992	XE SDWAN router stuck in boot loop after power-cycle due to replaystore file corruption
CSCvq97694	Local internet breakout (DIA) doesn't work on subinterfaces in IOS-XE SD-WAN 16.11.1a, 16.12.1b
CSCvr55738	spanning-tree mode rapid-pvst is not part of the default config on 16.12.1 XE SDWAN software anymore
CSCvr71786	Pairwise-keying configuration not enabled when configured through a vManage template

Resolved Bugs for Cisco SD-WAN Release 16.12.1d

Table 10: Resolved Bugs for Cisco SD-WAN Release 16.12.1d

Bug ID	Description
CSCvq67094	zbf drops hierarchical overlay traffic between spoke sites that go through hub ASR1001-X
CSCvq71921	ucode crash observed with ZBFW due to stuck thread processing data traffic
CSCvr27714	CSR+SDWAN on AWS will install default route in startup config which conflicts with some topologies

Resolved and Open Bugs for Cisco SD-WAN Release 16.12.1b

Resolved Bugs for Cisco SD-WAN Release 16.12.1b

Table 11: Resolved Bugs for Cisco SD-WAN Release 16.12.1b

Bug ID	Description
CSCvj84204	XE SDWAN: Control connections fail if DNS server is not reachable thru one TLOC interface in ECMP
CSCvk48972	Admin-tech failure via vManage for multiple Cisco XE SD-WAN Router platforms
CSCvm47984	ISR4331: 16.9.1: snmpwalk error - OID not increasing
CSCvm55520	C9407R - C9400-PWR-3200AC Power Supply goes into faulty state randomly ("n.a.")
CSCvn54741	Traffic not getting matched when using vsmart data policy

Bug ID	Description
CSCvn55971	Cisco XE SD-WAN Router: Locally sourced packets using wrong interface with ECMP
CSCvn63395	ASR-1002-HX crash at headend running 16.9.3
CSCvn71472	'snmp-server user' config shown as part of sdwan running config
CSCvn95901	High memory utilization on ISR1K C1111-8P platform
CSCvo00790	Cisco XE SD-WAN Router cli_template: Unable to move interface from global vpn
CSCvo31413	fman_fp crash after upgrading to build 201
CSCvo60765	SD-WAN router experiences an IOSd crash when connected to a controller
CSCvo69625	Increase IPSec tunnel limit to 200 by default without HSECk9 on ISR1k
CSCvo83361	XE SDWAN: add the error code support on XE SDWAN asr1k
CSCvo90556	XE SDWAN: NTP should try all available interfaces with ECMP
CSCvp08310	Not enough disk space to carry on configuration DB error when trying to install third image on ISR

Open Bugs for Cisco SD-WAN Release 16.12.1b

Table 12: Open Bugs for Cisco SD-WAN Release 16.12.1b

Bug ID	Description
CSCvj26197	Update statistics from Oecteon viptela code to platform
CSCvk72903	XE SDWAN-vDaemon: Sub-interface's control-local-properties shows state=UP even though it is admin-down
CSCvp15917	ciscosdwan.cfg located on the bootflash is ignored when bootstrapping a new router
CSCvp77035	vManage is pushing "negotiation auto" config to TenGigabitEthernet interface with optical SFPs
CSCvp79646	Unable to connect to vManage over the LTE interface when fail over executed from other transport.
CSCvq10160	Cellular IP is getting reset when primary transport interface Gi0/0/0 is shutdown.
CSCvq13727	CSR 1000v XE SDWAN instance keeps rebooting in AWS
CSCvq34185	Umbrella redirects not respecting local domain bypass list, it is not programmed to DP
CSCvq61835	interface cant be moved from vrf 0 to service vrf when it has ip address
CSCvq62993	Secondary Supervisor can't boot up after "redundancy force-switchover" command

Bug ID	Description
CSCvq67094	zbf drops hierarchical overlay traffic between spoke sites that go through hub ASR1001-X
CSCvq70071	flow data is not populated into /tmp/xml/fnf
CSCvq79547	Bootflash space exhaustion causing watchdog to trigger on ISR4351
CSCvq83612	Polaris 16.9 QFP crash due to a stuck thread

Controller Compatibility Matrix and Server Recommendations

For compatibility information and server recommendations, see Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations.

ROMmon Requirements Matrix

The following table lists the minimum ROMmon versions supported on the corresponding devices and releases:

Table 13: ROMmon Versions

Device	ROMmon Version for 16.10 Devices	ROMmon Version for 16.11 Devices	ROMmon Version for 16.12 Devices
ASR1000-X/HX	16.3(2r)	16.3(2r)	ASR1001-HX, ASR1002-HX, ASR1001-X: 16.9(4r ASR1002-X: 16.7(1r)
ISR 4000	16.7(4r)	16.7(4r)	16.12(1r)
ISR 1000	16.9(1r)	16.9(1r)	16.12(1r)

Table 14: Recommended Rommon Release for SD-WAN for Cisco ISR 4000 series Integrated Services Routers (Cisco ISR 4000)

Cisco IOS XE Release	Cisco 4321 ISR	Cisco 4321 ISR	Cisco 4331 ISR	Cisco 4351 ISR	Cisco 4431 ISR	Cisco 4451 ISR	Cisco 4461 ISR
Cisco IOS XE 16.9.x	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	—	—	—
Cisco IOS XE 16.10.x	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	—
Cisco IOS XE 16.11.x	16.7(5r)	16.7(5r)	16.7(5r)	16.7(5r)	16.12(2r	16.12(2r)	—
Cisco IOS XE 16.12.x	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)	16.12(2r)

Note ROMmon auto-upgrade is supported on the ISR 4000 series routers, beginning with 16.9.1 and all subsequent releases/throttles.

Note ROMmon auto-upgrade is supported on the ISR 1000 series routers, beginning with 16.10.3 and 16.12.1b.

Note For the ISR 1000 series routers, ROMmon version 16.8(1r) is not compatible with 16.10 releases and ROMmon version 16.9(1r) is not compatible with 16.9 releases. If an ISR 1000 series router is upgraded to a 16.10 release without auto-upgrade support, it is required that ROMmon be upgraded to 16.9(1r) or later by the user.

Related Documentation

- Release Notes for Previous Releases
- Software Installation and Upgrade for Cisco IOS XE Routers
- Software Installation and Upgrade for vEdge Routers
- Field Notices
- Deferral Notices
- Cisco Bulletins