Release Notes for Cisco IOS XE SD-WAN Release 16.10.x and Cisco SD-WAN Release 18.4.x

Last Modified: 2020-01-23

Release Notes for Cisco IOS XE SD-WAN Release 16.10.x and SD-WAN Release 18.4.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 RFP documentation, or language that is used by a referenced third-party product.

These release notes accompany the Cisco IOS XE SD-WAN Software Release 16.10, which provides SD-WAN capabilities for Cisco IOS XE SD-WAN devices, and the compatible Cisco SD-WAN Release 18.4 for Cisco vSmart Controller devices—including vBond orchestrators and vManage NMSs—and Cisco vEdge devices. These Release Notes include Cisco IOS XE SD-WAN Releases 16.10 through 16.10.6 and corresponding Releases 18.4 through 18.4.6.

Supported Devices

The Cisco IOS XE SD-WAN software runs on the following devices.

Table 1: Supported Devices and Versions

Device Family	Device Name
Cisco ASR 1000 Series Aggregation Services Routers	• ASR 1001-HX and ASR 1001-X • ASR 1002-HX and ASR 1002-X
Cisco ISR 1000 Series Integrated Services Routers	• C1111-8P, C1101-4P, C1111-8P LTE EA, and C1111-8P LTE LA • C1117-4P LTE EA, C1117-4P LTE LA • C1111-4P LTE EA, C1111-4P LTE LA, C1116-4P LTE EA, C1117-4P MLTE EA • C1111-4P, C1116-4P, C1117-4P, C1117-4PM, C1111X-8P (8GB RAM)

Device Family	Device Name
Cisco ISR 1000 Series Integrated Services Routers, with wireless services (WLanGigabitEthernet configuration required from vManage)	• C1111-8PWY (WiFi domain WY; Y = A, B, E, F, H, N, Q, R, Z) • C1111-8PLTEEAWX^*^ (WiFi domain WX; X = A, B, E, R)
Cisco ISR 4000 Series Integrated Services Routers	ISR 4221, ISR 4221-X, ISR 4321, ISR 4331, ISR 4351, ISR 4431, ISR 4451
Cisco 5000 Series Enterprise Network Compute System	• ENCS 5104, ENCS 5406, ENCS 5408 • ENCS 5412 with T1/E1 and 4G NIM modules
vEdge Routers	vEdge 100, vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000

Product Features

Below are the main product features added in Cisco SD-WAN Release 18.4 and Cisco IOS XE SD-WAN Release 16.10.

For Cisco IOS XE devices:

Cisco IOS XE SD-WAN device support all the following SD-WAN software features. For more information, see Software Installation and Upgrade for Cisco IOS XE SD-WAN device.

- Cisco SD-WAN security features
  - Enterprise Firewall with Application Awareness
  - Intrusion Prevention System
  - URL Filtering
  - DNS/Web-Layer Security
  - Umbrella auto-registration
  - Cloud: Local domain bypass for umbrella
- Onsite bootstrap process for SD-WAN edge routers.
- Template improvements: Network Design Builder, Device Profile Builder.
- vManage common template for multiple C1100 wireless SKUs.
- IPv6 on the service side + dual-stack
  - Dual-stack interfaces (Gig, sub-Interface, SVI, and loopback) on service side.
  - v6 routing protocols on service side: Static, BGP, route maps, inbound filtering, outbound filtering, v4 and v6 OMP redistribute, v4 and v6 redistribute between service VPN's.

    - IPv6 services features on service side: QOS, QOS policer on service side, QOS dscp re-write rule for inbound and outbound, ip name-server, ICMP redirects, VRRP, ACL, DHCP relay agent, SSH, traceroute, SNMP, logging server, MIB.

    - IPv6 addressing: Unicast (link-local, unique-local, and global), Anycast.

- Device life cycle (Monitoring Security Policies by Device).

For Cisco vEdge device:

- Adaptive FEC for optimizing TCP retransmits.
- ALG support for FTP client side with NAT— FTP ALG support with network address translation – SERVICE NAT, and Zone-Based Firewall (ZBFW).
- Template improvements: Network Design Builder, Device Profile Builder.
- Packet duplication for loss correction.
- SR-IOV vEdgeCloud support.

SD-WAN Features Not Supported on IOS XE Devices

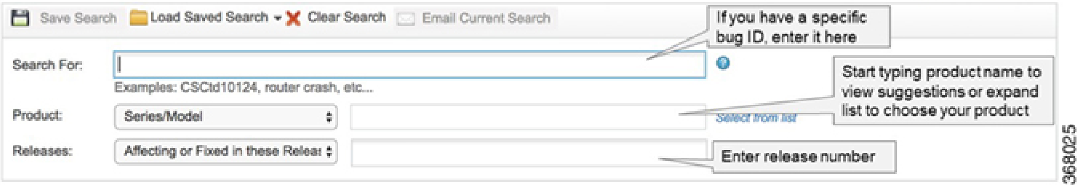
- Cloud Express service
- Cloud onRamp service
- Standard IPsec with IKE version 1 or IKE version 2 for service-side connections
- IPsec/GRE cloud proxy
- IPv6 on transport connections
- NAT pools on service-side connections
- Nat pools for DIA
- Service side NAT
- Reverse proxy
- Interface level policer (however, policer is supported through the interface ACL)
- Policy actions: local-tloc, local-tloc-list, remote-tloc (CSCvn67980), remote-tloc-list , mirror, log, service

Resolved and Open Bugs for Cisco IOS XE SD-WAN 16.10.x and Cisco SD-WAN 18.4.x

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.

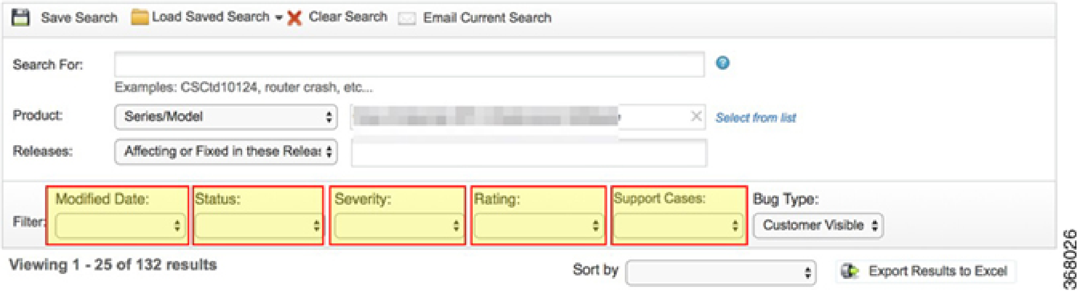


If you have a specific bug ID, enter it here

Start typing product name to view suggestions or expand list to choose your product

Enter release number

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



Resolved Bugs

All resolved bugs for this release are available in the Cisco Bug Search Tool through the Resolved Bug Search.

Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.6 and Cisco SD-WAN Release 18.4.6

Table 2: Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.6 and Cisco SD-WAN Release 18.4.6

Bug ID	Description
CSCvj14805	Cisco SD-WAN Solution Software Denial of Service Vulnerability
CSCvn61549	TACACS : vM generates malformed packets for all servers, except last one
CSCvo72974	vE5K performance drops significantly using loopback TLOC without 'bind' configuration
CSCvq11615	Route is not getting removed from the routing table even if the BFD is down.
CSCvq30332	fp-core watchdog failure on vEdge 5k running 18.4.1 (fp-um)
CSCvq35040	the configuration database is locked by session <id> system tcp git/vdaemon/vdaemon_misc.c
CSCvq53160	vManage: SSO authentication may not be possible after upgrade/reboot
CSCvq91658	Error in sending device list for Push vSmart List to vBond
CSCvq92007	MAC Authentication Bypass with radius server is not supported
CSCvr35741	DPI statistics database configuration memory increase
CSCvr51289	vtracker core while checking memory leaks when run with valgrind

Bug ID	Description
CSCvr52733	vedge frequently establishing control connections to the vBond even though it is in equilibrium
CSCvr86574	Updating template on vManage is causing IPSEC to flap.
CSCvr89182	ISR4331 fails upgrade to 16.12.1d and rollsback with ASR1001-HX identity
CSCvr89892	vdaemon crashes after change csr vbond ip
CSCvr92326	Cloud on Ramp not pushing configuration to vEdge-Cloud when adding Sites
CSCvs07518	vManage stores stale session and renders to j_security_check or last cached url
CSCvs10190	vEdge WLAN iPhone Wireless Clients dropping connection after 1-3 mins
CSCvs29732	core.chmgrd crashed on vedge upgrade.
CSCvs31128	vManage - no stats for IRB interfaces
CSCvs48535	%IPSEC-3-REPLAY_ERROR: + BFD down and drops IN_CD_COPROC_ANTI_REPLAY_FAIL
CSCvs58213	Vedge-5000:Auto IP feature support for feature parity.
CSCvs63167	Elasticsearch index purge should also delete red indices
CSCvs75634	16.12.3 ZBFW:Configuration database locked by vmanage-session
CSCvs75868	esg:destination overwhelmed messages are seen on sending high rate TCP traffic leading to iosd crash
CSCvs91182	vManage is pushing additional slash '\' with the banner line breaker
CSCvs96758	Not getting omp label on the edge devices which is causing traffic to take another link.
CSCvs97522	ISRv: default route/Next-hop ip address need to be validated at the attach window
CSCvt00090	vManage: vManage is unable to upgrade a vEdge cloud from 18.3.5 to 18.4.4
CSCvt01916	FTMd crash seen for Nutella with Dongle LTE model after multiple device reboot
CSCvt05575	SFTP to vManage is not working after upgrade to 20.1, 19.2
CSCvt06013	QoS map can't be assigned to sub-interface without Shaping rate - hit error
CSCvt22430	Certain configurations cause Dot1x to re-authenticate on a vedge running 18.4.302 with IRBs
CSCvt30224	Slash symbol cannot be used in a variable value of any device specific parameter scope in templates
CSCvt39342	ZBFW + IRB show severe packet loss
CSCvt42221	fp-um core observed on vEdge 5k device

Bug ID	Description
CSCvt43637	IOS-XE: SD-WAN: Improve Management port stability whilst under DoS Attacks
CSCvt54485	Nat over IPsec not working with ZBFW
CSCvt61421	vedge-cloud with SRIOV interfaces unable to receive IP packets more than 1496 bytes
CSCvt65197	vEdge SDWAN IPsec tunnel flapping due IKE packet drops
CSCvt65634	show system status shows CPU allocation is 3 when deployed with 2
CSCvt66319	Traffic stop sending across WAN when WAN link got unplugged and packet duplication is on :ISR1100-4G
CSCvt69001	Failed to detach the cEdge devices from wcm controller in vmanage Integration Page
CSCvt69529	Cisco SD-WAN vManage Software Denial of Service Vulnerability
CSCvt70360	Inconsistency between "show app dpi flows" output and Current flows count in show app dpi summary
CSCvt75034	vEdge cflowd core crash after interface config change
CSCvt91197	UTD subsystem crashes when UTD configs debugs are enabled on start-up
CSCvt92515	SIT : bfd sessions are not coming from source tloc where mcc is 0 and was working in earlier build
CSCvt93875	DNS response processing fails with Umbrella enabled after socket leak observed
CSCvu08599	vManage Feature hostname / location template should support special characters
CSCvu12536	Can't assign default router distance on sub-interface via vManage
CSCvu18773	[DyT]: Cxp doesn't compute loss/latency even with reachability due to Tracker status down
CSCvu21309	BFD sessions flap after multiple control connection flaps to the vSmart.
CSCvu29677	vManage misleading error regarding multitenancy in singe tenant environment cluster
CSCvu36501	"ftmd' crash on vEdge when cellular interface is present and "show interface" is executed
CSCvu40167	More specific route creates less specific aggregate in OMP
CSCvu40495	"show ipv6 interface" command returns incomplete IPV6 ADDRESS field
CSCvu49885	traffic flows are not load-balanced fairly across all available cores when using GRE tunnel in vedge
CSCvu50167	vSmart seeing crashes with high policy-queue.
CSCvu56004	Removing a data prefix list from one match condition removes it from all
CSCvu56405	Uploaded WAN-Edge list rejected, chassis tag missing

Bug ID	Description
CSCvu58050	SSO SAMLResponse redirect points to loginError.html unexpectedly
CSCvu69444	SNMP Query for Interface Description OID breaks if description is longer than 32 characters.
CSCvu71411	IKE IPSec: Generate an error message, if strongSwan can't execute rekey CLI
CSCvu74193	Vmanage displays error when "+:=@!"" is used in template variable
CSCvu74421	SNMP v3 walk is failing in vsmart and vedges
CSCvu79620	tunnel interface is admin up and oper down but local properties show admin and oper as down
CSCvu92440	Cisco PKI Root Certificates not installed in recent images
CSCvu98521	Device's are not booting up after a power outage
CSCvv07412	Device is unreachble, interfaces are showing as up
CSCvv10287	CoR probes working for O365 but failing for every other SaaS application
CSCvv17381	vEdge5000: control connection stuck in "Challenge" phase - Failed to create IdentityReqBlob
CSCvv19652	vEdge crashes with dbgd failed message when running speed test
CSCvv21757	Cisco SD-WAN vManage Software Privilege Escalation Vulnerability
CSCvv22275	Unable to see stats on vAnalytics in 18.4.5
CSCvv24320	Multiples vEdges crashing with "Software initiated - Daemon 'ftmd' failed"
CSCvv27194	vSmart crashes during vExpress run
CSCvv42376	Cisco SD-WAN Software Privilege Escalation Vulnerability
CSCvv54150	vedge_azurecloud_cloud_18_4_0 console logs are getting filled with HTTP logs
CSCvv54382	Unable to enable data stream option on the vManage in 18.4.5 version
CSCvv66595	dbgd crash observed on the vEdge router while running a speed test.
CSCvv89447	Cisco SD-WAN vManage cluster kills session after idle-timeout expires even when traffic is present
CSCvv90381	Vedge reversing the src and dst MAC instead of using its own src-mac.
CSCvw10824	Buffer pool leak seen on ISR1100-6G
CSCvu71921	Cisco SD-WAN Software Privilege Escalation Vulnerability
CSCvv02305	Cisco SD-WAN vManage Software XML External Entity Vulnerability

Bug ID	Description
CSCvv09807	Cisco SD-WAN Software Arbitrary File Creation Vulnerability
CSCvv21747	Cisco SD-WAN vManage Software Command Injection Vulnerability
CSCvv42398	Cisco SD-WAN Software Privilege Escalation Vulnerability
CSCvv42551	Cisco SD-WAN Software Privilege Escalation Vulnerability
CSCvv42616	Cisco SD-WAN vManage Software Cross-Site Scripting Vulnerability
CSCvv42620	Cisco SD-WAN vManage Cross-Site Scripting Vulnerability

Open bugs in Cisco IOS XE SD-WAN Release 16.10.6 and Cisco SD-WAN Release 18.4.6

Table 3: Open bugs in Cisco IOS XE SD-WAN Release 16.10.6 and Cisco SD-WAN Release 18.4.6

Bug ID	Description
CSCvo21728	vEdge forming duplicate control-connections after increasing number of cores on vSmart
CSCvp27158	CUE AA leg not cleared on ios after it does blind xfer to sip line
CSCvp87004	vManage GUI showing partial control status for vEdges having an LR interface after upgrade.
CSCvr84778	nping inconsistent on vmanage GUI vs CLI
CSCvr89780	policy with 127 char : can not configure src-port dest-port pkt-len with policy with 127 char.
CSCvs60659	vEdge x86: cFlowd flow setup burst on dedicate master core
CSCvs98101	Implement mechanism to synchronize information about peers between vSmarts
CSCvt07144	vSmart: omp peers do not come UP after "clear omp all" on vSmarts
CSCvt43318	Auto negotiate not working in vEdge2K
CSCvv04607	In vManage 20.1.1 UI bootstrap 3.2.0 is vulnerable to multiple medium CVE
CSCvv20699	Not able to push template due to stuck operation 18.4.5
CSCvv37343	WebHooks fails in vManage when more than one is configured
CSCvv47101	The request nms configuration-db configure command needs protection and documentation
CSCvv50436	vManage WebServer uses a hard coded self-signed certificate
CSCvv54844	ConfigDB not updating username/password
CSCvv61236	SNMP community not accepting exclamation ! in string

Bug ID	Description
CSCvv72515	vSmart (OMP) doesn't sync properly routes\TLOC information
CSCvv73959	PIM module showing down in show hw inventory
CSCvv88334	Email Notifications: with custom devices list a Number of 'Devices Attached' is blank when edit it
CSCvw01415	vManage API calls expose user password hashes
CSCvw03838	IPSEC session is getting stuck in IKE_INITIATE state
CSCvw28254	High CPU because of process vconfd_script_vmanage_list_stats.sh
CSCvw28477	version property of vEdge not populated on the vManage
CSCvw46957	Private AWS connections stop working after enabling AWS Cloud OnRamp for SaaS
CSCvw56871	18.3.8 vEdge crashing with Kernel panic, logs represent silent reboot
CSCvw64330	vEdge100B low upload speed for TCP traffic
CSCvw67332	vedgecloud with SRIOV (i40evf) intf receive max IP pkt 1468B when verifying CSCvt61421 with 18.4.6
CSCvw68364	When you add some app family in vManage GUI, additional shown in the Policy Preview and vSmart CLI
CSCvv21671	BGP neighbor will go UP even though the "shutdown neighbor" command is configured

Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.5 and Cisco SD-WAN Release 18.4.5

Table 4: Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.5 and Cisco SD-WAN Release 18.4.5

Bug ID	Description
CSCvj24700	Memory leak observed in the 'hman' process
CSCvk35589	An object group in use can be emptied by removing last item
CSCvs09893	AWS C5 instances of vmanage has very slow response and crashes with "hung_task"
CSCvm86435	confd_cli process is not terminated and hogging CPU
CSCvn80264	Certificate Expired Alarm for future date
CSCvq30348	fp-core watchdog falure on vEdge 5k running 18.4.1 tcpd crash
CSCvq93325	Cloud vEdge crash on bfdmgr_update_sla_mapping
CSCvr20826	OMP Feature Template - advertise ipv6 for vEdge leads to Config Preview Fail
CSCvr39991	vEdge 1000 - FP crash with Zone Based Firewall and IRB config

Bug ID	Description
CSCvr44637	ASR1k - OMP prefix SLA_CLASS has HW handle: (nil) (not-created)_with GROUP-ID
CSCvr52320	vEdge2K Crashed with resolvd failed
CSCvr52733	vedge frequently establishing control connections to the vBond even though it is in equilibrium
CSCvr60723	Multiple fp-um crashes seen on vEdge cloud on 18.3.5
CSCvr67907	vEdge5k: FTMD vmRSS leak on SIT basic regression - From 254MB to 350+MB
CSCvr73195	Cellular interface not coming up after user authentication failure
CSCvr79487	Real-Time OMP Advertised routes taking longer on 18.4 and higher versions than 17.2 and lower
CSCvr82612	vManage provide incorrect failure message when device memory is low.
CSCvr89892	vdaemon crashes after change csr vbond ip
CSCvr95187	vmanage admin tech generation failed after 30 minutes for vedge1k/vedge2k, device takes longer time
CSCvs04363	VPN label is changing upon vEdge reboot
CSCvs09160	Redistribution from OSPF to BGP is failing in vEdge when policy is being applied
CSCvs09341	fman_fp crash seen with traffic soak
CSCvs09799	When sub interfaces(with SAME Higher bits) are configured with IPv6, only 1 is active.
CSCvs13262	vedge-cloud receive locks up in openstack virtio environment
CSCvs14302	vEdge 5k on the 18.4.302 code stops forwarding packets over the 10 Gig interfaces
CSCvs14659	Bring down ge0/0 is not causing ipsec interface to report down
CSCvs14717	IPsec tunnel stuck in IKE_INIATE with vEdge not initiating IKE packets.
CSCvs16700	vEdge iPerf speed test -r option is not working as expected
CSCvs20881	vManage devices change mode API is taking long time with scale
CSCvs21703	VManage UI Unresponsive or very slow in 18.3.8; Full GC (Allocation Failure)
CSCvs25859	Software install skipped because vManage thinks it is "already in progress"
CSCvs26107	vManage displays circuits even when the bfd session is not up between the circuits
CSCvs26265	Data collection is slow on vManage after enabling vAnalytics
CSCvs27694	sub-inteface is still seen in running-config after delete from vmanage

Bug ID	Description
CSCvs31193	ZBFW policy re-ordering in vManage fails when pushed to XE SDWAN router
CSCvs37431	gateway showing mandatory for different prefix in update device template
CSCvs39434	vManage/vSmart system status(CPU/Memory) stuck at Zero percent
CSCvs45364	vEdge - NAT Fail Lookup on return traffic through Standard IPSec Tunnel
CSCvs45820	Partial connections in vmanage dashboard when interface is admin down by user
CSCvs49495	CLI template push fails on vEdge if it contains special character "&" in the template
CSCvs53861	19.2.099 vmanage system template showing invalid value for decimal GPS values
CSCvs56652	SD-WAN router may delete newly created SA in a specific case
CSCvs61972	Deleting a rules under FW policy when multiple rules are configured, fails
CSCvs68356	vedge-cloud with NAT/cflowd, forwarding performance is degraded by 50%
CSCvs68498	vManage the user ip display the local link ip address in AUDIT LOG
CSCvs70954	vManage/vSmart upgrade to 18.4.4 and OMP Process is taking too much time to clear.
CSCvs70961	vmanage gui not accessible as /opt/data is 100% full. App server down
CSCvs71811	Vmanage goes OOM after upgrade to 19.2.1 java.lang.OutOfMemoryError: Java heap space
CSCvs75313	Failed to initialized dot1x interface when ip address was change for the server
CSCvs76945	OMP feature template - Not able to select Advertise ipv6
CSCvs82091	request csr upload fails with lost connection
CSCvs83609	Dbgd daemon crashed with signal 6 after running vEdge packet capture
CSCvs83794	Ipv6 tunnel interface is not getting dhcp ip after upgrade from 19.3 to 20.1 in amazon instances.
CSCvs84918	Traffic simulation is not working properly on 19.2.1
CSCvs88834	ZBFW TCP state needs to move to TIMEWAIT when a vaild RST packet is received
CSCvs90207	On cEDGE all the BFD session flap if there is a control connection flap to vmanage
CSCvs93379	vManage config preview is timing out on large config.
CSCvs94762	vEdge not generating reboot event
CSCvs95487	vEdge 2k with 17.2.8 see high CPU because of process vconfd_script_vmanage_list_stats.sh

Bug ID	Description
CSCvs98586	Skip SDWAN tunnel encapsulated packets in UTD DP and set inspected flag when skipping inspection
CSCvt16595	XE SDWAN routers experience slow memory leak over time in 'ncsshd' process
CSCvt16841	Vedge ipsec tunnel stops passing traffic during high load and rekey
CSCvt21897	SDWAN/vEdge: vEdge PIM traffic loss and eventually PIM crash
CSCvt42611	Performance is very low with subinterfaces on vEdge5k
CSCvt46779	Route export not working as desired during failover testing
CSCvt61717	Route export not working as expected during failover testing
CSCvt71865	SNMP not working on tunnel interface and to loopback interface in vpn 0.
CSCvt74507	RDP Session resets with 802.1x running with default reauth and inactivity values
CSCvv42576	Cisco SD-WAN vManage Cypher Query Language Injection Vulnerability
CSCvw08529	Cisco SD-WAN vManage Cypher Query Language Injection Vulnerability

Open bugs in Cisco IOS XE SD-WAN Release 16.10.5 and Cisco SD-WAN Release 18.4.5

Table 5: Open bugs in Cisco IOS XE SD-WAN Release 16.10.5 and Cisco SD-WAN Release 18.4.5

Bug ID	Description
CSCvn76844	vBond DNS resolution may fail in ECMP environment
CSCvp46172	vEdge: default route is not getting installed even after arp is learnt when def gw is not pingable
CSCvq35040	the configuration database is locked by session <id> system tcp git/vdaemon/vdaemon_misc.c
CSCvq91658	Error in sending device list for Push vSmart List to vBond
CSCvr09310	vManage should be able to work with cEdge banners in the same way as with vEdges
CSCvr35741	DPI statistics database configuration memory increase
CSCvr45900	Software Repository file upload: Remote server must take full URL including filename
CSCvr51289	vtracker core while checking memory leaks when run with valgrind
CSCvr86574	Updating template on vManage is causing IPSEC to flap.
CSCvr89182	ISR4331 fails upgrade to 16.12.1d and rollsback with ASR1001-HX identity
CSCvr92326	Cloud on Ramp not pushing configuration to vEdge-Cloud when adding Sites

Bug ID	Description
CSCvs48535	%IPSEC-3-REPLAY_ERROR: + BFD down and drops IN_CD_COPROC_ANTI_REPLAY_FAIL
CSCvs75634	16.12.3 ZBFW:Configuration database locked by vmanage-session
CSCvs96758	Not getting omp label on the edge devices which is causing traffic to take another link.
CSCvs97179	VEDGE 100M VZ LTE last resort circuit came UP randomly
CSCvs97522	ISRv: default route/Next-hop ip address need to be validated at the attach window
CSCvs99153	Not able to configure logging host <ipv4-addr> vrf <vrf-name>
CSCvt01532	SD-WAN router running 16.10.3 crashes with cpp_cp_svr fault
CSCvt01916	FTMd crash seen for Nutella with Dongle LTE model after multiple device reboot
CSCvt06013	QoS map can't be assigned to sub-interface without Shaping rate - hit error
CSCvt39342	ZBFW + IRB show severe packet loss
CSCvt42221	fp-um core observed on vEdge 5k device
CSCvt54485	Nat over IPsec not working with ZBFW
CSCvt61421	vedge-cloud with SRIOV interfaces unable to receive IP packets more than 1496 bytes
CSCvt63771	vManage generates 'Failed to create input variables' error after feature template edit
CSCvt65197	vEdge-100m IPsec Tunnel Flapping due internal DROPs
CSCvt65298	VRRP issue with vEdge-5k
CSCvt65634	show system status shows CPU allocation is 3 when deployed with 2
CSCvt76335	vedge frequently establishing control connections to the vBond even though it is in equilibrium
CSCvt85171	[SIT]: Generation of Admin Tech on 18.4.5 vedge mips platform fails
CSCvt87370	Memory spikes seen for dca when fetching large amounts of data and sending to server.
CSCvt91197	UTD subsystem crashes when UTD configs debugs are enabled on start-up
CSCvt93875	DNS response processing fails with Umbrella enabled after socket leak observed
CSCvu01693	vManage creating IPS signature update tasks for routers in staging mode and without security policy
CSCvs10190	vEdge WLAN iPhone Wireless Clients dropping connection after 1-3 mins
CSCvs31128	vManage - no stats for IRB interfaces

Bug ID	Description
CSCvt70360	Inconsistency between "show app dpi flows" output and Current flows count in show app dpi summary
CSCvu08599	vManage Feature hostname / location template should support special characters
CSCvu14047	vManage throws HTTP error 500 randomly for API requests
CSCvu18220	vManage Feature hostname / location template should support special characters
CSCvt92515	SIT : bfd sessions are not coming from source tloc where mcc is 0 and was working in earlier build
CSCvp44731	Unable to ping to the virtual gateway IP when VRRP is configured on 10G sub-interfaces on vEdge5K
CSCvt66319	Traffic stop sending across WAN when WAN link got unplugged and packet duplication is on :ISR1100-4G
CSCvu98521	Device's are not booting up after a power outage
CSCvv23993	vEdge 2000: Software initiated - Daemon 'zebra' failed

Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.4 and Cisco SD-WAN Release 18.4.4

Table 6: Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.4 and Cisco SD-WAN Release 18.4.4

Bug ID	Description
CSCvi80775	Decouple buffer allocation for egress queues from the interface speed negotiated
CSCvk51661	memory leak in vdaemon
CSCvn24727	Large number of out-of-order packets seen with vEdge5k and vEdge-Cloud
CSCvn67202	Cisco SD-WAN Solution Packet Filtering Bypass Vulnerability
CSCvo21464	MIPS images writing a bunch of FP printf() output to main console
CSCvo53544	Admin-tech Failure in vManage for Cisco XE SD-WAN Router
CSCvp00165	OSPF Feature Template : Area nssa summary and translate not configured on CSR
CSCvp24427	SDAVC fails to complete activation
CSCvq02230	vEdge-5000 running 18.4.1 hitting DPI-out-of-memory causing the memory to climb to 100%
CSCvq12913	vEdge1000 crashed even after applying the 18.4.101 ES image
CSCvq30332	fp-core watchdog failure on vEdge 5k running 18.4.1 (fp-um)
CSCvq34350	vEdge Service side interface not responding to inter-vpn/inter-zone pings from local host

Bug ID	Description
CSCvq62238	Transport tracker is not going down when the default route via the interface is removed
CSCvq65977	Rollback timer doesn't work as expected, broken in 18.4 code
CSCvq67476	ikev2 dpd retransmit always 1s and fails after one retry with "giving up after 1 retransmits"
CSCvq75671	IPSEC interface down alarms are not cleared sometimes
CSCvq86066	vEdge 5K crash with kernel panic
CSCvq88184	a vEdge will crash if the WAN interface loses its IP via DHCP
CSCvq97954	Cellular interface doesn't get an IP address when brought up through the pnp workflow
CSCvq98760	Unable to add device specific value in bgp feature template in 18.4.3
CSCvr18076	ISR4K automatically reboot everytime after placing "commit".
CSCvr32117	connected routes are not distributed in OMP for VRF number greater than 512
CSCvr47452	KVM: vEdgeCloud is displaying swap_dup: Bad swap file entry after Upgrade to RHEL 7.6 OPS 10.21
CSCvr54141	Hostname is truncated in the event logs on the vManage
CSCvr63960	Vmanage Doesn't Allow Configuring IPv6 Static Route Under VPN512 for Cedge
CSCvr79487	Real-Time OMP Advertised routes taking longer on 18.4 and higher versions than 17.2 and lower
CSCvr91093	Error occurs when try to collect BFD link status by API
CSCvs01637	ms_teams is missing from the list of office365 cloudexpress
CSCvs13262	vedge-cloud receive locks up in openstack virtio environment
CSCvs14444	Packets drops observed when primary transport is coming back up on the router.
CSCvj72674	Adding dscp to AAR match clears counters that don't seem to increment
CSCvn65879	Hostname out of sync in IOS and confd after reload
CSCvp34370	After upgrade to 18.3.5 static routes with a nh ip on a shut SUB interface are redistributed to OMP.
CSCvq07958	Cloud OnRamp for SAAS doesn't work when sending via 3rd Party IKE IPSEC Tunnel (Zscaler)
CSCvq75871	IPSec SA receives anti-replay error for all packets for NAT session flap sometimes
CSCvq76075	HMAC failure due to incorrect stale nat fixup entry for the ipsec session after symnat session flap

Bug ID	Description
CSCvr42619	No ARP ping packets generated after loading xe-sdwan 16.10.3a image on asr1k
CSCvr91255	improve handling of fragment failures with zone based firewall
CSCvr98412	FP core seen in fp_do_tx_pkt_duplication with vedge packet duplication testcases

Open bugs in Cisco IOS XE SD-WAN Release 16.10.4 and Cisco SD-WAN Release 18.4.4

Table 7: Open bugs in Cisco IOS XE SD-WAN Release 16.10.4 and Cisco SD-WAN Release 18.4.4

Bug ID	Description
CSCvp07124	FP core watchdog fail on vEdgecloud 18.4.1 running on Azure.
CSCvr35176	Device is crashing constantly when TCP optimization is enabled.
CSCvr52680	Stale vManage certs present on the vManage after we factory reset it and install a new cert
CSCvr76398	Wrong order of operations when changing TenGe subinterface on ASR1k to different vlan id
CSCvr84372	VPN0 interface won't come up on vbond KVM instance on RHEL7.5
CSCvm86435	confd_cli process is not terminated and hogging CPU
CSCvs08871	vManage 19.2.099 shows Invalid value if GPS Lat/Long is float
CSCvs88582	Data Policy names needs to be under 26 characters if you plan to upgrade to 18.4.4
CSCvt95983	vEdge Cloud: vEdge on Azure may go into a bootloop state after an upgrade from 18.4.302 to 19.2.2
CSCvp44731	Unable to ping to the virtual gateway IP when VRRP is configured on 10G sub-interfaces on vEdge5K

Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.3b and Cisco SD-WAN Release 18.4.303

Table 8: Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.3b and Cisco SD-WAN Release 18.4.303

Bug ID	Description
CSCvk77287	vEDGE 1000 Reboot - ospf crash
CSCvn02180	confd died on upgrading from 18.3.X to 18.4 on 100b
CSCvo33693	vEdge-1000 using DIA and ZBFW having issues intermittenly with iframes of specific site after zbfw s
CSCvp11416	cEdge - Template attach fails for a cedge device if theres a central policy with cflowd activated

Bug ID	Description
CSCvp52043	vSmart Crashing: Core files "Daemon 'vdaemon_inst_0' failed" getting generated on the vSmart
CSCvp90232	cEdge omp aggregate-only gives unpredictable results
CSCvq61835	interface cant be moved from vrf 0 to service vrf when it has ip address
CSCvq70691	Configuring IPv6 DNS Server through vManage fails for vEdge platforms
CSCvq70727	Configuration fails to push with "Bad CLI switchport access vlan name ATM-1, location 2" error
CSCvq97694	Local internet breakout (DIA) doesn't work on subinterfaces in IOS-XE SD-WAN 16.11.1a, 16.12.1b
CSCvr02735	template hardening - allow encrypted fields with more than 31 chars
CSCvr15242	omp routes redistributed into ospf are advertised back into omp causing a routing loop
CSCvr19249	vEdge performs NAT translation to public source port 0 or overlaps ports when all ports exhausted

Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.3a and Cisco SD-WAN Release 18.4.302

Table 9: Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.3a and Cisco SD-WAN Release 18.4.302

Bug ID	Description
CSCvn24727	Large number of out-of-order packets seen with vEdge5k and vEdge-Cloud
CSCvo08423	[Vistraprint] GUI unresponsive after upgrade to 18.3.4
CSCvp02442	Connectivity to the service side of vEdgecloud in Azure is lost when sending lot of tcp packets.
CSCvp10364	cEdge router crash because of viptela_start_sh fault
CSCvp13167	vEdge5000: control connection stuck in "Challenge" phase with TPM lockup
CSCvp50832	Network > Device> Real Time options wont be displayed if we login with SSO
CSCvq02230	vEdge-5000 running 18.4.1 hitting DPI-out-of-memory causing the memory to climb to 100%
CSCvq10160	Cellular IP is getting reset when primary transport interface Gi0/0/0 is shutdown.
CSCvq12913	vEdge1000 crashed even after applying the 18.4.101 ES image
CSCvq41120	Banner Feature Template : Device Template Push Fails when banner template is removed
CSCvq46984	BFD goes down on a Cisco XE SDWAN Router if it is behind symmetric NAT & the ports change frequently

Bug ID	Description
CSCvq56875	Failure in configuration push to a cedge when we move tunnel-interface from parent to sub-interface
CSCvq61992	ISR1100 not booting up after power cycle and gets stuck in boot loop - replaystore file corruption
CSCvq62764	Passive FTP connection fails when connections are routed through DIA link of VEdge
CSCvq67094	zbf drops hierarchical overlay traffic between spoke sites that go through hub ASR1001-X
CSCvq68449	QFP ucode crash while processing large packet with NBAR enabled
CSCvq86066	vEdge 5K crash with kernel panic
CSCvq88184	a vEdge will crash if the WAN interface loses its IP via DHCP
CSCvq98760	Unable to add device specific value in bgp feature template in 18.4.3
CSCvr27373	nesd crash on XE SDWAN router when pushing large configuration
CSCvq60546	sriov support for ixgbevf xl520 adapters in openstack environments
CSCvp24427	SDAVC fails to complete activation

Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.3 and Cisco SD-WAN Release 18.4.3

Table 10: Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.3 and Cisco SD-WAN Release 18.4.3

Bug ID	Description
CSCvk06180	vQos - Packets buffered too long in the interface queue
CSCvk48972	Admin-tech failure via vManage for multiple Cisco XE SD-WAN Router platforms
CSCvk79079	SSO Requires browser cache to sign in after first login
CSCvm56707	'default-information originate' not disabled in VPN0
CSCvm97332	config commit operation fails on ISRv on 5406 with error ext2_lookup:deleted inode referenced
CSCvn18683	qos: can't change bandwidth allocation for the class in the qos-map
CSCvn22546	vManage needs to adjust memory threshold for warnings on Cisco XE SD-WAN Router platform
CSCvn32354	"Factory reset all" makes the Cisco XE SD-WAN Router inaccessible. Cant boot image fr bootflash
CSCvn38443	Cloudexpress Errors - Failed to enable sites for CloudExpress
CSCvn38487	vManage does not generate proper AAA configuration for Cisco XE SD-WAN Router

Bug ID	Description
CSCvn44400	Login banner does accept banners over 238 characters
CSCvn45732	Device crashing if we unconfigure the NTP on the device
CSCvn55971	Cisco XE SD-WAN Router: Locally sourced packets using wrong interface with ECMP
CSCvn56474	After swapping tunnel-destination among 2 gre-intfs, one of the gre-intf does not get programmed
CSCvn59626	NTP template attach fails with a non default vrf and source interface configured
CSCvn66750	vManage - VMAN does not gen proper config for DHCP static binding w/ hostname specified
CSCvo00790	Cisco XE SD-WAN Router cli_template: Unable to move interface from global vpn
CSCvo02422	class-queue mappings are never pushed until there are class references in local policy
CSCvo02433	'SNMP has locked CDB' error while trying to edit a user group in vManage
CSCvo02607	SVM: transaction log can grow up to 25 GB in size
CSCvo02748	packets sourced with loopback interface and that are exceeding mtu on the service side are not fragm
CSCvo26474	vEdge-1000 reboot with 18.4.0 (FP core watchdog fail)
CSCvo26926	Not able to push CLI template due to kafka error (Too many open files)
CSCvo31413	fman_fp crash after upgrading to build 201
CSCvo48927	WAN Interface stays down after an upgrade or reload of a vEdge 5000
CSCvo61990	'show system statistics diff' does not work
CSCvo68150	'allow-service bgp' on vEdge Cloud not working as expected
CSCvo68788	sdwan: vManage should not push ip nbar protocol-discovery on loopback0
CSCvo68842	Google applications access issues when using DIA with app-list match in data-policy
CSCvo69041	SVM: server config file is empty
CSCvo69105	vManage does not handle chassis id in uppercase when activating vEdge Cloud
CSCvo70767	Device may show out of sync after a control connection flap
CSCvo74585	Cisco IOS-XE SD-WAN router with factory 16.9.2 software is shown as vEdgeCloud on vManage
CSCvo77664	UTD: Server response is leaked if URL verdict response is late
CSCvo79535	template push failure on ISR4331(16.10) due to discrepancy in setting "weight" (tunnel) parameter

Bug ID	Description
CSCvo94092	vManage in 18.4.1 is unable to push banner to Cisco XE SD-WAN Router 16.10.2
CSCvp13167	vEdge5000: control connection stuck in "Challenge" phase with TPM lockup
CSCvp13833	snmp-server trap-source configuration is not generated for Cisco XE SD-WAN Router by vManage
CSCvp16606	sdwan isr receiving any SOO changes AD to 252
CSCvp18231	DHCP relay not forwarding dhcp request packets.
CSCvp19188	vManage generates incorrect Cisco XE SD-WAN Router config for DHCP excluded-address ranges
CSCvp21016	vEdge FTMD crash
CSCvp25994	CVM: OOM - vManage GUI becomes very sluggish. Tasks start to time out
CSCvp34862	Unable to import Database with TACACS login details
CSCvp37418	vManage is not sending filtered queries while displaying real time cflowd data from the vEdge.
CSCvp38066	ZTP: All production ztp servers vdaemon cored at the same time
CSCvp46023	vEdge dropping DHCP offer when source ip and dhcp-helper does not match.
CSCvp51861	DHCP ip pool config get removed after upgrade from 18.4.0.1 to 18.4.1
CSCvp51863	Ping intermittently fails because vEdge sends wrong ICMP ident in the header.
CSCvp52217	FTMD crash seen on a vE1K node
CSCvp61972	After reload of v5k with cloud-qos-service-side configured throughput drops and RED drops seen
CSCvp63629	Cellular modem is rebooting frequently
CSCvp65817	"default-information originate" stays in the config even if "originate" is disabled in the template
CSCvp65969	Tunnel group-id does not work as expected causing traffic loss
CSCvp67098	Can't update existing Localized Policy with new Access Control List
CSCvp68381	Unable to push policy to the vSmart after upgrade of the vManage from 18.3.5 to 18.4.101.
CSCvp70217	SVM: NMS app-server fails to start
CSCvp77191	vManage not processing statistics from device when vAnalytics is enabled for large deployments
CSCvp77533	Template failure results in 'Failed to finish the task' after 30 min

Bug ID	Description
CSCvp78025	Stuck 'Send to Controllers' task on vManage blocking other tasks
CSCvp78629	Template fails due to physical interface removal after upgrade
CSCvp79222	ZBFW policy sequences not displayed in vManage UI after upgrade to 18.4 or higher from 18.3
CSCvp86310	Cisco XE SD-WAN Router unable to inject packets when traffic is destined to it
CSCvp96887	Failed to attach template to Cisco XE SDWAN Rtr if qos-map name changed after policy-map is attached
CSCvq02087	BFD sessions not forming between a Cisco XE SD-WAN Router behind symmetric NAT & a vEdge with NO NAT
CSCvq07823	Control connection drops even with high timeout with low-bandwidth-link on vEdge
CSCvq12443	tracker doesn't work for DIA in case of centralised data-policy used
CSCvq13368	packet loss seen with rapid pings on nat interface, drop reason showing as map-db add failures
CSCvq22687	<ip name-server vrf 1> configuration not saved upon upgrade from 16.9 to 16.10
CSCvq42802	vedge : DIA Traffic Policy restrict doesn't work as expected
CSCvq46984	BFD goes down on a Cisco XE SDWAN Router if it is behind symmetric NAT & the ports change frequently
CSCvq50896	BFD session not coming up on tloc-extension interface due to wrong UID
CSCvq54726	continuous nat-pool exhausted failure leads to map-db leak
CSCvq56813	vSmart allowing 5 SLA classes under policy causing problem pushing that to vEdges
CSCvq61992	XE SDWAN router stuck in boot loop after power-cycle due to replaystore file corruption

Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.2 and Cisco SD-WAN Release 18.4.1

Table 11: Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.2 and Cisco SD-WAN Release 18.4.1

Bug ID	Description
CSCvj50058	The vManage DPI screen displays a DIA graph for a vEdge router on which local Internet exit is not c
CSCvj88473	cEdge doesn't revert configuration after WAN interfaces shut from vManage
CSCvj90293	nesd crash on show platform software trace message nesd R0 on TSN
CSCvk72985	Device goes out-of-sync during network flap and never attempts template push after it is reachable

Bug ID	Description
CSCvm61034	Template push cEdge failing with: (ERR): Bad CLI source Loopback0, location 16
CSCvm68397	NTP source interface configuration is not genrated by vManage
CSCvm70027	GC allocations errors causing GUI to be unresponsive
CSCvn77852	{StaticPageTitle} {static error message } seen on select device page
CSCvn78404	Unable to push policy to vSmart after upgrading from 18.3.4 to 18.4.0

Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.1 and Cisco SD-WAN Release 18.4.0

Table 12: Resolved bugs in Cisco IOS XE SD-WAN Release 16.10.1 and Cisco SD-WAN Release 18.4.0

Bug ID	Description
CSCvk77480	An '&' character in the organization-names breaks template pushes
CSCvm46954	vEdge 5K Template Attach - Null Error Msg
CSCvk78359	vEdge Crashed when issuing a "show ospf ... " command
CSCvm68056	Incorrect VRF name mapping for NTP source VPN in vManage
CSCvi59726	Cisco SD-WAN vManage SQL Injection Vulnerabilities
CSCvk28609	Cisco SD-WAN vManage SQL Injection Vulnerabilities
CSCvk28656	Cisco SD-WAN vManage SQL Injection Vulnerabilities
CSCvk28667	Cisco SD-WAN vManage SQL Injection Vulnerabilities
CSCvi59632	Cisco SD-WAN vManage Software Path Traversal Vulnerability
CSCvk28549	Cisco SD-WAN vManage Software Path Traversal Vulnerability

Open Bugs

All open bugs for this release are available in the Cisco Bug Search Tool through the Open Bug Search.

The following list contains open bugs for Cisco IOS XE SD-WAN Release 16.10.1 through 16.10.3 andCisco SD-WAN Release 18.4.0 through 18.4.3.

Bug ID	Description
CSCvi80775	Decouple buffer allocation for egress queues from the interface speed negotiated
CSCvj26197	Update statistics from Oecteon viptela code to platform
CSCvj29165	ENH - all user groups for cEdge are configured with same privilege 15
CSCvj82776	Incorrect tag for omp routes

Bug ID	Description
CSCvk27129	The requirement to shutdown Dialer interface before its deletion causes an issue for vManage
CSCvk48972	Admin-tech failure via vManage for multiple Cisco XE SD-WAN Router platforms
CSCvk72903	cEdge-vDaemon: Sub-interface's control-local-properties shows state=UP even though it is oper-down
CSCvn38487	vManage does not generate proper AAA configuration for Cisco XE SD-WAN Router
CSCvn76615	source-interface mapping is missing in vmanage for tacacs and radius server group.
CSCvo34208	Memory leak in SMAND
CSCvo40967	linux_iosd memory goes up on ISR1100 over extended soak
CSCvo88281	Config Diffs not aligned properly in vManage due to line spacing
CSCvp09156	NTP issue on Cisco XE SD-WAN Router - cannot specify source interface in service VPN
CSCvp50832	Network > Device> Real Time options wont be displayed if we login with SSO
CSCvq62764	Passive FTP connection fails when connections are routed through DIA link of VEdge
CSCvr32117	connected routes are not distributed in OMP for VRF number greater than 512
CSCvp44731	Unable to ping to the virtual gateway IP when VRRP is configured on 10G sub-interfaces on vEdge5K

Compatibility Matrix and Server Recommendations

For compatibility information and server recommendations, see Cisco SD-WAN 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 16.9 Devices	ROMmom Version for 16.10 Devices
ASR	16.3(2r)	16.3(2r)
ISR 4000	16.7(3r)	16.7(4r)
ISR 1000	16.8(1r)	16.9(1r)

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.

The ISRv router is running the minimum required version of the CIMC and NFVIS software, as shown in the table below:

Hardware Platform	CIMC	NFVIS
ISRv	3.2.9	3.12.3 FC3

Important Notes, Known Behavior, and Workaround

Known Behaviour - Hardware

The following are known behaviors of the hardware:

- On vEdge 1000 routers, support for USB controllers is disabled by default. To attach an LTE USB dongle to a vEdge 1000 router, first attach the dongle, and then enable support for USB controllers on the vEdge router by adding the system usb-controller command to the configuration. When you enter this command in the configuration, the router immediately reboots. Then, when the router comes back up, continue with the router configuration. Also for vEdge 1000 routers, if you plug in an LTE USB dongle after you enable the USB controller, or if you hot swap an LTE USB dongle after you enable the USB controller, you must reboot the router in order for the USB dongle to be recognized. For information about enabling the USB controller, see USB Dongle for Cellular Connection.

- For vEdge 2000 routers, if you change the PIM type from a 1-Gigabit Ethernet to a 10-Gigabit Ethernet PIM, or vice versa, possibly as part of an RMA process, follow these steps:

  1. Delete the configuration for the old PIM (the PIM you are returning as part of the RMA process).
  2. Remove the old PIM, and return it as part of the RMA process.
  3. Insert the new PIM (the PIM you received as part of the RMA process).
  4. Reboot the vEdge 2000 router.
  5. Configure the interfaces for the new PIM.

- On a vEdge 5000 router, you cannot enable TCP optimization by configuring the tcp-optimization-enabled command.

- Cisco IOS XE SD-WAN device with the SFP-10G-SR module do not support online insertion and removal (OIR) of this module.
- Use of port-channels on the Service Side VPN is not supported on Cisco IOS XE SD-WAN devices.
- Bridge Domain Interface (BDI) is not supported on the Cisco ASR1000.

Known Behaviour - Software

The following are known behaviors of the software:

Cellular Interfaces

- On a vEdge 100m-NA and 100m-GB routers, when you configure profile 1 for a wireless WAN, you might see the error "Aborted: 'vpn 0 interface cellular0 profile': Invalid profile 1 : APN missing". [VIP-31721].
- When configuring cellular attach-profile and data-profile on Cisco IOS XE routers running the XE SD-WAN software, you must use the default profile ID.
- The vEdge 100wm router United States certification allows operation only on non-DFS channels.
- When you are configuring primary and last-resort cellular interfaces with high control hello interval and tolerance values, note the following caveats:
    - When you configure two interfaces, one as the primary interface and the other as the last-resort interface, and when you configure a high control hello interval or tolerance values on the last-resort interface (using the hello-interval and hello-tolerance commands, respectively, the OMP state indicates init-in-gr even though it shows that the control connections and BFD are both Up. This issue was resolved in Release 16.2.3. However, the following caveats exist:

      — You can configure only one interface with a high hello interval and tolerance value. This interface can be either the primary or the last-resort interface.

      — In certain cases, such as when you reboot the router or when you issue shutdown and no shutdown commands on the interfaces, the control connections might take longer than expected to establish. In this case, it is recommended that you issue the request port-hop command for the desired color. You can also choose to wait for the vEdge router to initiate an implicit port-hop operation. The request port-hop command or the implicit port hop initiates the control connection on a new port. When the new connection is established, the stale entry is flushed from the vSmart controllers.
    - If the primary interface is Up, as indicated by the presence of a control connection and a BFD session, and if you configure a last-resort interface with higher values of hello interval and tolerance than the primary interface, if you issue a shutdown command, followed by a no shutdown command on the last-resort interface, the last-resort interface comes up and continuously tries to establish control connections. Several minutes can elapse before the operational status of the last-resort interfaces changes to Down. If this situation occurs, it is recommended that you issue a request port-hop command for the desired color.
    - If you have configured a primary interface and a last-resort interface that has higher hello interval and tolerance values than the primary interface, and if the last-resort interface has control connections to two vSmart controllers, if you issue a shutdown command, followed by a no shutdown command on the last-resort interface, a control connection comes up within a reasonable amount of time with only one of the vSmart controllers. The control connection with the second vSmart controller might not come up until the timer value configured in the hello tolerance has passed. If this situation occurs, it is recommended that you issue a request port-hop command for the desired color.

- When you activate the configuration on a router with cellular interfaces, the primary interfaces (that is, those interfaces not configured as circuits of last resort) and the circuit of last resort come up. In this process, all the interfaces begin the process of establishing control and BFD connections. When one or more of the primary interfaces establishes a TLOC connection, the circuit of last resort shuts itself down because it is not needed. During this shutdown process, the circuit of last resort triggers a BFD TLOC Down alarm and a Control TLOC Down alarm on the vEdge router. These two alarms are cleared only when all the primary interfaces lose their BFD connections to remote nodes and the circuit of last resort activates itself. This generation and clearing of alarms is expected behavior.
- For cellular interface profile, the profile number can be 0 through 15. Profile number 16 is reserved, and you cannot modify it.

Configuration and Command-line Interface

- When you upgrade to Release 17.2 from any prior Cisco SD-WAN release, the CLI history on the Cisco vEdge device is lost. The CLI history is the list of commands previously entered at the CLI prompt. You typically access the history using the up and down arrows on the keyboard or by typing Ctrl-P and Ctrl-N. When you upgrade from Release 17.2 to a later software release, the CLI history is maintained.
- When you issue the **request reset configuration** command on a vEdge Cloud router, a vManage NMS, or a vSmart controller, the software pointer to the device's certificate might be cleared even though the certificate itself is not deleted. When the device reboots and comes back up, installation of a new certificate fails, because the certificate is already present. To recover from this situation, issue the **request software reset** command.

Control and BFD Connections

- When a vBond orchestrator, vManage NMS, or vSmart controller goes down for any reason and the vEdge routers remain up, when the controller device comes back up, the connection between it and the vEdge router might shut down and restart, and in some cases the BFD sessions on the vEdge router might shut down and restart. This behavior occurs because of port hopping: when one device loses its control connection to another device, it port hops to another port in an attempt to reestablish the connection. For more information, see the Firewall Ports for Cisco SD-WAN Deployments article. Two examples illustrate when this might occur:
    - When a vBond orchestrator goes down for any reason, the vManage NMS might take down all connections to the vEdge routers. The sequence of events that occurs is as follows: when the vBond orchestrator crashes, the vManage NMS might lose or close all its control connections. The vManage NMS then port hops, to try to establish connections to the vSmart controllers on a different port. This port hopping on the vManage NMS shuts down and then restarts all its control connections, including those to the vEdge routers.
    - All control sessions on all vSmart controllers go down, and BFD sessions on the vEdge routers remain up. When any one of the vSmart controllers comes back up, the BFD sessions on the routers go down and then come back up because the vEdge routers have port hopped to a different port in an attempt to reconnect to the vSmart controllers.
- When a vEdge router running Release 16.2 or later is behind a symmetric NAT device, it can establish BFD sessions with remote vEdge routers only if the remote routers are running Release 16.2 or later. These routers cannot establish BFD sessions with a remote vEdge router that is running a software release earlier than Release 16.2.0.

- When you add or remove an IPv4 address on a tunnel interface (TLOC) that already has an IPv6 address, or when you add or remove an IPv6 address on a TLOC that already has an IPv4 address, the control and data plane connections for that interface go down and then come back up.
- Release 16.3 introduces a feature that you can use to configure the preferred tunnel interface to use to exchange traffic with the vManage NMS. In the vManage NMS, you configure this on cellular, Ethernet, and PPP Interface feature templates, in the vManage Connection Preference field under Tunnel Interface. In the CLI, you configure this with the vmanage-connection-preference command. The preference value can be from 0 through 8, with a lower number more preferable. The default value is 5. If you set the preference value to 0, that tunnel interface is never used to exchange traffic with the vManage NMS, and it is never able to send or receive any overlay network control traffic.

  With this configuration option, there is one situation in which you can accidentally configure a device such that it loses all its control connections to all Cisco vSmart Controller devices (the vManage NMSs and the vSmart controllers). If you create feature templates and then consolidate them into a device template for the first time, the NMS software checks whether each device has at least one tunnel interface. If not, a software error is displayed. However, when a device template is already attached to a device, if you modify one of its feature templates such that the connection preference on all tunnel interfaces is 0, when you update the device with the changes, no software check is performed, because only the configuration changes are pushed to the device, not the entire device template. As a result, these devices lose all their control connections. To avoid this issue, ensure that the vManage connection preference on at least one tunnel interface is set either to the default or to a non-0 preference value.

Interfaces

- On virtual interfaces, such as IRB, loopback, and system interfaces, the duplex and speed attributes do not apply, and you cannot configure these properties on the interfaces.
- When a vEdge router has two or more NAT interfaces, and hence two or more DIA connections to the internet, by default, data traffic is forwarding on the NAT interfaces using ECMP. To direct data traffic to a specific DIA interface, configure a centralized data policy on the vSmart controller that sets two actions—nat and local-tloc color. In the local-tloc color action, specify the color of the TLOC that connects to the desired DIA connection.
- When configuring interfaces for an IOS XE router using one of the VPN Interface feature configuration templates, you must spell out the interface names completely. For example, you must type GigabitEthernet0/0/0. Also, you must define all the interfaces in the router even if you are not using them so that they are configured in the shutdown state and so that all default values for them are configured.
- For IOS XE routers that have a DSLAM module plugged in, you must include the VPN Interface DSL PPPoA or the VPN Interface DSL PPPoE feature configuration template in the device configuration template to successfully configure the routers from vManage NMS.

IPv6

- You can configure IPv6 only on physical interfaces (ge and eth interfaces), loopback interfaces (loopback0, loopback1, and so on), and on subinterfaces (such as ge0/1.1).
- For IPv6 WAN interfaces in VPN 0, you cannot configure more than two TLOCs on the vEdge router. If you configure more than two, control connections between the router and the Cisco vSmart Controller might not come up.
- IPv6 transport is supported over IPsec encapsulation. GRE encapsulation is not supported.

- You cannot configure NAT and TLOC extensions on IPv6 interfaces.
- HMAC failure due to incorrect stale nat fixup entry for the ipsec session after symnat session flap.
- DHCPv6 returns only an IPv6 address. No default information is accepted. IPv6 router solicitation and router advertisement messages are not processed.

IRB

- On integrated routing and bridging (IRB) interfaces, you cannot configure autonegotiation.

NAT

- When you reboot a vSmart controller, the BFD sessions for all symmetric NAT devices go down and come back up. This is expected behavior.

Policy

- In policy definitions, any application list or application family list that you define with an app-list option cannot have more than 10 items per list.
- NAT DIA with matching app-list is not supported offically. All Cisco vEdge devices and Cisco IOS XE SD-WAN devices share the same limitation. Please evaluate other options like the Cloud Express feature for SAAS DCA capabilities.

Routing Protocols

- When a vEdge router transport interface is using an old IPv6 SLAAC address for control connections or BFD sessions, or both, the IP address used for control connections and BFD might become out of sync with the actual IPv6 address. This situation can happen when the IPv6 address that SLAAC advertises from the gateway router changes suddenly and the old IPv6 address has not first been invalidated. As a workaround, if the router has no mechanism to invalidate older prefixes when the IPv6 prefix changes, first remove the router-advertisement configuration on the default gateway router and then change the IPv6 address. To resolve this problem when it occurs on a vEdge router, shut down the interface and then restart it; that is, issue a shutdown command, followed by a no shutdown command.
- When you configure OSPF using a vManage NMS device configuration template, the configuration of an NSSA area or a stub area and the configuration of an area range are not pushed to the router when you attach the device configuration template to the router. As a workaround, configure these parameters in CLI mode on the router, from the vManage Tools ► SSH Terminal screen, using the OSPF area and range configuration commands.

Security

- It is recommended that you use IKE Version 2 only with Palo Alto Networks and Ubuntu strongSwan systems. Cisco SD-WAN has not tested IKE Version 2 with other systems.

SNMP

- When you configure an SNMP trap target address, you must use an IPv4 address.

- The Cisco SD-WAN interface MIB supports both 32-bit and 64-bit counters, and by default sends 64-bit counters. If you are using an SNMP monitoring tool that does not recognize 64-bit counters, configure it to read 32-bit MIB counters.
- On a vEdge router, if you perform an snmpwalk getnext request for an OID for which there is no information, the response that is returned is the next available instance of that OID. This is the expected behavior.

T1/E1

- If you wish to change the card and controller type on the device, you must first remove the previously configured card and controller and reboot the device.
- You cannot configure rollback or load override features on a multilink interface.
- PPP multilink QoS is currently not supported in the VPN Interface Multilink template.
- PPP multilink NAT is currently not supported in the VPN Interface Multilink template.
- For a vEdge Cloud VM instance on the KVM hypervisor, for Cisco SD-WAN Releases 16.2.2 and later, it is recommended that you use virtio interfaces. For software versions earlier than Release 16.2.2, if you are using the Ubuntu 14.04 or 16.04 LTS operating system, you can use IDE, virtio, or virtio-scsi interfaces.

vManage NMS

- On a Cisco vEdge device that is being managed by a vManage NMS system, if you edit the device's configuration from the CLI, when you issue the commit command, you are prompted to confirm the commit operation. For example:

  ```
  vEdge(config-banner)# commit
  ```

  The following warnings were generated:

  ```
  'system is-vmanaged': This device is being managed by the vManage. Any configuration
  changes to this device will be overwritten by the vManage. Proceed? [yes,no]
  ```

  You must enter either yes or no in response to this prompt.

  During the period of time between when you type commit and when you type either yes or no, the device's configuration database is locked. When the configuration database on a device is locked, the vManage NMS is not able to push a configuration to the device, and from the vManage NMS, you are not able to switch the device to CLI mode.
- The members of a vManage cluster rely on timestamps to synchronize data and to track device uptime. For this time-dependent data to remain accurate, do not change the clock time on any one of the vManage servers of the cluster after you create the cluster.
- When you use the vManage Maintenance ► Software Upgrade screen to set the default software version for a network device, that device must be running Release 16.1 or later at the time you set the default software version. If the network device is running Release 15.4 or earlier, use the CLI request software set-default command to set the default software version for that device.
- When you are using a vManage cluster, when you are bring up a new vManage NMS in the cluster, use an existing vManage NMS to install the certificate on the new vManage NMS.

- In vManage feature configuration templates, for the passwords listed below, you cannot enter a cleartext password that starts with $6 or $8. You can, however, use such passwords when you are configuring from the CLI.
  - Neighbor password, in the BGP feature configuration template.
  - User password, in the Cellular Profile feature configuration template.
  - Authentication type password and privacy type password, in the SNMP feature configuration template.
  - RADIUS secret key and TACACS+ secret key, in the System feature configuration template.
  - IEEE 802.1X secret key, in the VPN Interface Ethernet feature configuration template.
  - IPsec IKE authentication preshared key, in the VPN Interface IPsec feature configuration template.
  - CHAP and PAP passwords, in the VPN Interface PPP Ethernet feature configuration template.
  - Wireless LAN WPA key, in the WiFi SSID feature configuration template.
- PPP CHAP is currently not supported in the VPN Interface Multilink template.
- PPP multilink fragmentation is currently not supported in the VPN Interface Multilink template.
- If a serial interface is bundled into a multilink interface, you cannot remove it from the vManage NMS.
- After you attach the VPN Interface Multilink template to a device, you cannot detach it from the device.

Licensing

- The maximum aggregated cyrpto throughput for the ISR 1000 series routers is 250 Mbps. HSECK9 license is required to achieve IPSec tunnel scale greater than 100 on ISR1000 series routers.
- Base licensing package of AX needs to be enabled for IOS-XE SDWAN ISRv during VM deployment on the ENCS portal.

Upgrade to SD-WAN Software Release from Cisco SD-WAN Release 18.3 to Cisco SD-WAN Release 18.4

Note For details on upgrading the Cisco IOS XE SD-WAN software, see Software Installation and Upgrade for Cisco IOS XE SD-WAN device.

Note For details on upgrading the Cisco SD-WAN, see Software Installation and Upgrade for Cisco IOS XE SD-WAN device.

Note Cisco SD-WAN releases starting with Releases 18.4.5, 19.2.2, and 20.1.1 have a security lockout. When any of these software versions (or later) are installed and activated on a device, a 30-day timer is set for the removal of any old images that were previously installed on the device. After the timer expires, the old images are deleted. For example, if you install and activate Release 18.4.5, a 30-day timer starts on the previously installed Release 19.2.1 image, but not on Release 19.2.2. Similarly if you install and activate Release 19.2.2, a 30-day timer starts on the previously installed Release 18.4.4 image, but not on Release 18.4.5.

You can continue to activate an older image that is already installed, before the 30-day timer runs out. If the device restarts before the 30-day timer expires, the timer is reset.

See following commands for more information:

- **request software secure-boot set**- Makes the system immediately delete old images* without waiting the 30 days.
- **request software secure-boot status**- Tells you whether or not you have old images* installed.
- **request software secure-boot list**- Prints a list of all old images* that are installed.

*old images= before releases 18.4.5, 19.2.2, and 20.1.1

Note You cannot install a Release 17.2 or earlier image on a Cisco vEdge device that is running Release 18.2.0 or later. This is the result of security enhancements implemented in Release 18.2.0. Note that if a Release 17.2 or earlier image is already present on the router, you can activate it.

Note When the vManage NMS is running Release 18.4.x, all Cisco IOS XE SD-WAN device in the overlay network must run Release 16.10.1 or later.

Note If you are upgrading to 18.4.4, Data Policy names need to be under 26 characters.

To upgrade your Cisco vEdge device to Cisco SD-WAN Release 18.4:

1. In vManage NMS, select the **Maintenance** > **Software Upgrade screen.**
2. Upgrade the controller devices to Release 18.4 in the following order:
    a. Upgrade the vManage NMSs in the overlay network.
    b. Upgrade the vBond orchestrators.
    c. Upgrade the vSmart controllers.
3. Select the **Monitor** > **Network screen.**
4. Select the devices you just upgraded, click the Control Connections tab, and verify that control connections have been established.
5. Select the **Maintenance** > **Software Upgrade** screen, and upgrade the vEdge routers.

Note After you upgrade software on a vManage NMS to any major release, you can never downgrade it to a previous major release. For example, if you upgrade the vManage NMS to Release 18.4, you can never downgrade it to Release 18.3 or to any earlier software release.

The major release number consists of the first two numbers in the software release number. For Cisco IOS XE SD-WAN software, 16.10 is a major release, and 16.10.1 denotes the initial release of 16.10. For Cisco SD-WAN, 18.4 and 18.3 are examples of major releases. Releases 18.4.0 and 18.3.0 denote the initial releases, and Releases 18.3.1 and 18.2.1 are maintenance releases.

Note When you upgrade from 16.9.x to 16.10.x, bootflash for 4GB platforms in 16.10.3 needs free space of 400MB besides having up to 3 images. Keeping space in bootflash is recommended beyond 400 MB for error free install/upgrades. The software reset command is not supported when the image is downloaded through USB and TFTP. Support of software reset is available only through bootflash.

Upgrade from Cisco IOS XE SD-WAN Release 16.2 and Earlier Software Releases

Because of software changes in Release 16.3, you must modify the router configuration as follows before you upgrade from Release 16.2 or earlier to Release 18.3:

- Use max-control-connections 0 instead of the no control-connections command in tunnel-interface configuration mode. The no control-connections command has been deprecated and has no effect on releases 17.2 and later.
- You can no longer configure RED drops on low-latency queuing (LLQ; queue 0). That is, if you include the policy qos-scheduler scheduling llq command in the configuration, you cannot configure drops red-drop in the same QoS scheduler. If your vEdge router has this configuration, remove it before upgrading to Release 17.2. If you do not remove the RED drop configuration, the configuration process (confd) fails after you perform the software upgrade, and the Cisco vEdge device roll back to their previous configuration.
- For vEdge 2000 routers, you can no longer configure interfaces that are not present in the router. That is, the interface names in the configuration must match the type of PIM installed in the router. For example, if the PIM module in slot 1 is a 10-Gigabit Ethernet PIM, the configuration must refer to the proper interface name, for example,10ge1/0, and not ge1/0. If the interface name does not match the PIM type, the software upgrade fails. Before you upgrade from Release 16.2 or earlier to Release 17.2, ensure that the interface names in the router configurations are correct.