Release Notes for Cisco IOS XE SD-WAN Release 16.9.x and Cisco SD-WAN Release 18.3.x

First Published: 2019-04-15

Release Notes for Cisco IOS XE SD-WAN Release 16.9.x and Cisco SD-WAN Release 18.3.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 16.9, which provides SD-WAN capabilities for Cisco IOS XE SD-WAN routers, and the compatible SD-WAN Software Release 18.3 for controller devices—including vSmart controllers, vBond orchestrators, and vManage NMSs—and vEdge routers. These release notes accompany Cisco IOS XE SD-WAN Releases 16.9.1 through 16.9.6, and Cisco SD-WAN Releases 18.3.0 through 18.3.8.

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, C1111-8P LTE EA, and C1111-8P LTE LA • C1117-4P LTE EA, C1117-4P LTE LA
Cisco 4000 Series Integrated Services Routers	ISR 4221, ISR 4321, ISR 4331, ISR 4351
ENCS 5412 with T1/E1 and 4G NIM modules	ISRv

Product Features

All the Cisco IOS XE routers support all SD-WAN software features except the following:

- 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
- Interface level QoS Policer
- NAT pools on service-side connections
- Reverse proxy

- Cisco router interfaces—The SD-WAN software runs with DSL, 4G LTE, and multilink router interfaces. See VPN Interface DSL PPPoA, VPN Interface DSL PPPoE, VPN Interface Multilink, and VPN Interface SVI.
- Cloud OnRamp—Within each cloud, AWS or Azure, you can map a transit VPC/VNet in one account to a host VPC/VNet in a different account. See Cloud OnRamp with AWS and Cloud OnRamp with Azure.
- CoS marking—You can mark data traffic with 802.1p class of service (CoS) values. See Configuring Localized Data Policy and Policies.
- Email notifications of alarms—You can configure the vManage server to send email notifications to an email address or to a webhook URL when selected alarms are generated. See Configure Email Notifications for Alarms and Alarms.
- NAT pools—You can configure pools of public IP address and map them to private IP addresses. See Configuring Transport-Side NAT.
- Single sign-on (SSO)—You can enable single sign-on for the vManage NMS to allow users to be authenticated using an external identity provider. This feature complies with the SAML Version 2.0 standard. See Settings.
- Software image security—When you install a Release 18.3.1 or later version of the software on a Viptela device, after one week, all Release 18.1.x and earlier software images are automatically removed from the device, and you cannot reinstall them. (Release 18.2.x images are not removed.) This feature, which was added in Release 18.3.1, improves device security. In addition, after one week, a new, more secure boot loader is installed on hardware vEdge routers. The specific behavior is as follows: the device waits for one week's worth of seconds (604,800 seconds) from when a Release 18.3.x software version starts on the device, and it then removes any older images and installs the new boot loader. For this to occur, the device must be up continuously for one week. If you reboot the device before one week elapses, the one-week timer starts from the beginning; the uptime is not cumulative. If you do not want to wait one week, you can manually initiate removal of older software images and loading of the secure boot loader by issuing the request software secure-boot set command.
- SR-IOV vEdgeCloud support—You can run vEdgeCloud on SR-IOV supported hardware.

- VRRP virtual MAC addresses—VRRP complies with RFC 5798 with regards to virtual MAC addresses and gratuitous ARP requests. See Configuring VRRP.

Compatibility Matrix

Table 2: Compatibility Matrix

Controllers	ENCS/ISR/ASR	ISRv	vEDGE
18.3.5	16.9.4	16.9.4 with NFVIS 3.9.1FC1 or NFVIS 3.9.2-FC4	17.2 or higher

Upgrade to SD-WAN Software Release 18.3

Note For details on upgrading the Viptela software, see Software Installation and Upgrade for vEdge Routers.

Note You cannot install a Release 17.2 or earlier image on a vEdge router 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 18.3.1, all Cisco IOS XE SD-WAN routers in the overlay network must run Release 16.9.2.

To upgrade your vEdge router to SD-WAN Software Release 18.3:

1. In vManage NMS, select the **Maintenance** > **Software Upgrade screen.**
2. Upgrade the controller devices to Release 18.3 in the following order:
   a. First, upgrade the vManage NMSs in the overlay network.
   b. Then, upgrade the vBond orchestrators.
   c. Next, 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 18.3, you can never downgrade it to Release 18.2 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, 16.9 is a major release, and 16.9.1 denotes the initial release of 16.9. For SD-WAN software, 18.3 and 18.2 are examples of major releases. Releases 18.3.0 and 18.2.0 denote the initial releases, and Releases 18.3.1 and 18.2.1 are maintenance releases.

Note After you install Release 18.3 on any Viptela controller device or on a vEdge router, you cannot install an older version of the software (that is, Release 18.2 or earlier) on the device. If an older software image is already present on the device and you remove it from the device, either on the vManage **Maintenance** > **Software Repository** screen or using the request software delete CLI command, you cannot re-install the older software image. However, if an older software image is present and you do not remove it, you can downgrade to it and, if necessary, you can install another older software version.

Upgrade from 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:

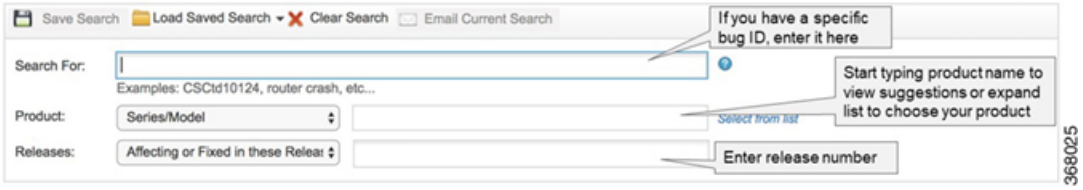
- You can no longer configure RED drops on low-latency queuing (LLQ; queue 0). That is, if you include the `policy qos-scheduler scheduling llq` command in the configuration, you cannot configure drops red-drop in the same QoS scheduler. If your vEdge router has this configuration, remove it before upgrading to Release 17.2. If you do not remove the RED drop configuration, the configuration process (confd) will fail after you perform the software upgrade, and the Viptela devices will 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 will fail. Before you upgrade from Release 16.2 or earlier to Release 17.2, ensure that the interface names in the router configurations are correct.

Resolved and Open Bugs in Cisco IOS XE SD-WAN Release 16.9.x and Cisco SD-WAN Release 18.3.x

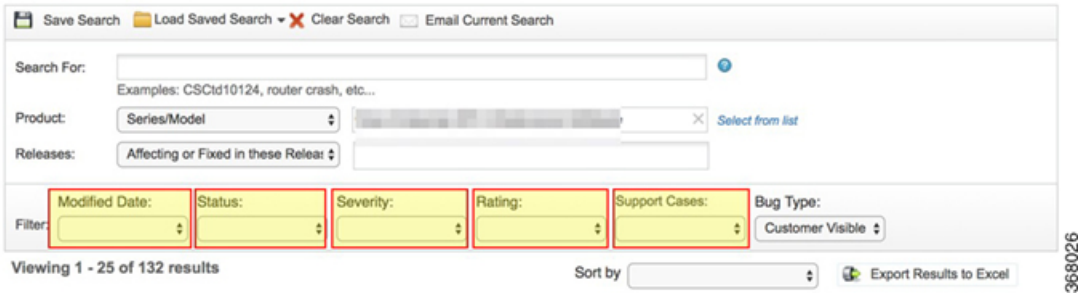
About the Cisco Bug Search Tool

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.



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 SD-WAN Release 18.3.8

Table 3: Resolved bugs in Cisco SD-WAN Release 18.3.8

Caveat ID Number	Description
CSCvq12443	Tracker doesn't work for DIA in case of centralised data-policy used
CSCvp02442	Connectivity to the service side of vEdge cloud in Azure is lost when sending lot of tcp packets
CSCvp73890	vEdge dropping VRRP packets if destination is its own sub interface on primary VRRP router
CSCvq45201	Regression: OSPF route policy filters out NAT default route instead of OSPF routes in 18.3.6
CSCvq47707	vManage: ClusterManagement REST API Call may not provide correct info for the NMS services running
CSCvq54726	Continuous nat-pool exhausted failure leads to map-db leak
CSCvq60197	Transport interface tracker does not work properly with endpoint-dns-name
CSCvp42169	Configurations show out of order in vManage and indicate changes when none were made
CSCvp50832	Network > Device > Real Time options wont be displayed if we login with SSO
CSCvp51863	Ping intermittently fails because vEdge sends wrong ICMP ident in the header

Caveat ID Number	Description
CSCvq34368	vManange Cluster: vManage Details gives an error
CSCvq80393	Zscaler tunnel failure (because NAT selects public port 0)
CSCvq89475	MTT Network > Device > Real Time options wont be displayed if we login with SSO
CSCvp70217	SVM: NMS app-server fails to start

Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.6 and Cisco SD-WAN Release 18.3.7

Table 4: Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.6 and Cisco SD-WAN Release 18.3.7

Caveat ID Number	Description
CSCvi46909	Cisco SD-WAN Solution Command Injection Vulnerabilities
CSCvi59723	Cisco SD-WAN Solution Command Injection Vulnerabilities
CSCvi59724	Cisco SD-WAN Solution Command Injection Vulnerabilities
CSCvi69886	Cisco SD-WAN Solution Privilege Escalation Vulnerability
CSCvp96612	SNMP traps on vedge not egressing out of the SNMP source

Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.5 and Cisco SD-WAN Release 18.3.6

Table 5: Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.5 and Cisco SD-WAN Release 18.3.6

Caveat ID Number	Description
CSCvn71845	QoS doesn't work properly on vEdge 100 cellular interfaces
CSCvo05590	Bulk edit of feature template attached to ~500 ISR devices takes 5 min per device for config gen
CSCvo08423	[Vistraprint] GUI unresponsive after upgrade to 18.3.4
CSCvo48927	WAN Interface stays down after an upgrade or reload of a vEdge 5000
CSCvo61990	'show system statistics diff' does not work
CSCvo69105	vManage does not handle chassis id in uppercase when activating vEdge Cloud
CSCvo88281	Config Diffs not aligned properly in vManage due to line spacing
CSCvo99766	UI: Issue with type 8 hashes in CLI templates
CSCvp09156	NTP issue on Cisco XE SD-WAN Router - cannot specify source interface in service VPN
CSCvp18231	DHCP relay not forwarding dhcp request packets.

Caveat ID Number	Description
CSCvp30369	NAT translation is not happening for return traffic
CSCvp33762	Unable to commit if there are more than 24 sub-interface under same vrrp group.
CSCvp34862	Unable to import Database with TACACS login details
CSCvp46023	vEdge dropping DHCP offer when source ip and dhcp-helper does not match.
CSCvp73223	C1111 router crashing even after ROMMON downgrade
CSCvp82758	Edit vmanage from local host to ip before cluster addition failing

Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.5 and Cisco SD-WAN Release 18.3.5

Table 6: Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.5 and Cisco SD-WAN Release 18.3.5

Caveat ID Number	Description
CSCvj50058	The vManage DPI screen displays a DIA graph for a vEdge router on which local Internet exit is not c
CSCvj63407	%Viptela-DC1-vEdge-1-FTMD-3-ERRO-1000011: FP Core 1 Died. Core file recorded at /var/crash/core.fp1.
CSCvj72674	Adding dscp to AAR match clears counters that don't seem to increment
CSCvk12352	Config Diff is not lining up properly
CSCvk67444	/config/policy/app-visibility: the 'when' expression "/viptela-system:system/viptela-system:personal
CSCvk72985	Device goes out-of-sync during network flap and never attempts template push after it is reachable
CSCvm26033	Cisco SD-WAN Privilege Escalation Vulnerabilities
CSCvm40554	DPI summary stats show no active flows incorrectly after switching in-n-out of OOM
CSCvm51895	vManage fails to push template to cEdge with error "sleep interrupted"
CSCvm60731	5k performance degradation between 18.3.0 and 18.3.1
CSCvm61034	Template push cEdge failing with: (ERR): Bad CLI source Loopback0, location 16
CSCvm72402	"Commit and-quit" exits to routers enable prompt instead of SD-WAN mode enable prompt
CSCvm73159	Fetching devices for cloudexpress returns empty list and IndexOutOfBoundsException in log
CSCvm82508	vManage: VPN Ethernet interface feature template with ICMP redirect will generate error message, can

Caveat ID Number	Description
CSCvm87869	vManage: cEdge BGP per-neighbor next-hop-self is in a feature template, but not in the config-previe
CSCvm92803	00019181 - In 18.3.1 we have replay-window set to 8192 but when doing a show security-info command,
CSCvn09989	BFD configurations not applied to cEdge/SDWAN-XE router
CSCvn10265	FIB is missing the NH programming causing route absence for the traffic
CSCvn11751	after adding enterprise root cert, master_root.crt is not in syn on cluster setup
CSCvn11753	vman_templates: Error on config preview "Template edit request has expired: Please try again" if te
CSCvn12443	Sequence matching on port range and protocol causes DIA to fail
CSCvn20682	feature template for ISR1K won't set interface to no autonegotiation
CSCvn23034	New IPsec session is not initiated on tunnel-destination change
CSCvn32404	vEdge5k control not coming up with vBond
CSCvn34872	prefix-list changes are not causing OSPF route filtering reevaluation (refresh)
CSCvn35840	vedge2k rebooted because FP core died
CSCvn42513	cEdge - Unable to change OSPF cost on interface using template
CSCvn50535	Control status dashboard shows wrong data under partial connections
CSCvn50624	Help icon redirects to older viptela documentation URL
CSCvn54776	Vmanage clustering port number missing under neo4j.conf after upgrade from 17.2.7 to 18.3.4
CSCvn64023	vManage does not generate proper config for cEdge OSPF stub and NSSA areas
CSCvn64054	vManage should not generate "max-metric router-lsa" for cEdge if it's not configured in template
CSCvn66750	vManage - VMAN does not gen proper config for DHCP static binding w/ hostname specified
CSCvn74107	vManage does not produce proper configuration for localized route-policy default action "Accept"
CSCvn74826	Add support for next-hop interface in static route definition in vManage for cEdge
CSCvn77309	CVM: Control Status shows incorrect info
CSCvn78560	vManage VPN Ethernet interface template: Loopback interface is not pushed to cEdge
CSCvn79173	CVM: DPI stats went into bad state

Caveat ID Number	Description
CSCvn81667	ENH - vManage not pushing "low-bandwidth-link" configuration to a cEdge.
CSCvn82645	Application list CLI vs vM UI inconsistency
CSCvo00514	Template push fail with "fail to finish task" for 140 ISR devices.
CSCvo09244	Devices stuck in scheduled state when editing feature template with 200 devices

Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.3 and Cisco SD-WAN Release 18.3.4

Table 7: Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.3 and Cisco SD-WAN Release 18.3.4

Caveat ID Number	Description
CSCvj43259	Cflowd: APP ID Export in IPFIX packets with SNMP MIB table (PLMREQ 974)
CSCvj79568	Throughput drop when using vlan tagged interfaces for transport
CSCvk45719	IP NAT route command is not getting generated while configuring DIA via vManage template
CSCvk64741	When show log messages is issued Ctrl C does not terminate the output
CSCvk65202	cEdge GPS location is not updated through vManage feature template
CSCvm40434	Interface is not getting programmed in VPN 0 when we move from Auto IP to static IP address assignme
CSCvm42884	vEdge100m Crash when workstation requests DHCP adress
CSCvm49899	ve100m throughput drop when QOS config is applied
CSCvm60972	add support to expose internal fp_dump commands to customer
CSCvm64917	OSPF router-ID with multi-tenant vmanage is getting messed up
CSCvm65707	vManage: TLOC-Extension configuration is not generated for cEdge
CSCvm66521	NAT Overload (PAT) assigns the same translated source port for first two consecutive hosts
CSCvm68469	No allow service https is pushed as allow service in feature template
CSCvm79118	00019228- Telefonica Business Solutions - can't access the vmanage via https, but ssh works. vManage
CSCvm79174	Vmanage should send individual vlan configuration during (CSCvm70375)template push when vlan range i
CSCvm82501	Memory leak with ttmd leads to segmentation fault
CSCvm82919	ftmd crash with 'request admin-tech'

Caveat ID Number	Description
CSCvm92358	vManage: cEdge qos rewrite rule is in the template, but not in the config-preview
CSCvm94862	GE0/4 on vEdge100M doesn't accept packets with size greater than default mtu (1500)
CSCvm98291	vManage creates Gig sub-interfaces when TenGig subs are defined for OSPF
CSCvm98802	"ip helper-address" configuration is not being pushed from the vManage to the cEdge when we use sub-
CSCvn02849	vEdge 5K: vDaemon crash while attempting to establish control connections at bootup
CSCvn04178	vEdge does not translate the source-ip of ICMP return packet
CSCvn16681	Pings above 1472 on vE5K fail on 10G interfaces
CSCvn22423	vEdge100m-VZ Crashing after enabling cflowd and DPI. error fp_proc_flow.

Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.3 and Cisco SD-WAN Release 18.3.3.1

Table 8: Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.3 and Cisco SD-WAN Release 18.3.3.1

Caveat ID Number	Description
CSCvk45719	IP NAT route command is not getting generated while configuring DIA via vManage template
CSCvk65202	cEdge GPS location is not updated through vManage feature template
CSCvm48856	[GreatWall EFT]: Changing the device models in a Feature Template is NOT working
CSCvm49430	VManage fail to generate the BGP per neighbor route-map configuration
CSCvm53683	vManage shouldn't generate "ip vrf forwarding 0" configuration for TACACs in global table for cEdge
CSCvm65707	vManage: TLOC-Extension configuration is not generated for cEdge
CSCvm80695	AAA auth-order doesn't update based on template changes in vManage
CSCvm92487	Loss Correction Delete / Remove button inoperable in Data Policy
CSCvm92710	with default NGOAM xc hb-interval, xc tunnel ports continuously flap, MTS build up CFS & CFS core
CSCvm96824	ENH: vmanage AAA template source-interface only accepting physical interfaces for cEdge
CSCvm98291	vManage creates Gig sub-interfaces when TenGig subs are defined for OSPF
CSCvm98802	"ip helper-address" configuration is not being pushed from the vManage to the cEdge when we use sub-
CSCvm99099	Cannot create VPN Interface Ethernet Template

Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.3 and Cisco SD-WAN Release 18.3.3

Table 9: Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.3 and Cisco SD-WAN Release 18.3.3

Caveat ID Number	Description
CSCvk14637	ZTP should block15.4.4 vEdge from joining 17.2.x overlay
CSCvk44883	[SF][D12]: port 12 from VLAN 513 should be removed from microinit of LC switch
CSCvk45719	IP NAT route command is not getting generated while configuring DIA via vManage template
CSCvk65155	snmpwalk timing out for viptela-omp for table ompRoutesTableFamilyEntriesReceivedAttributesOriginMet
CSCvk75135	Unable to accept vrrp control packets in a data policy
CSCvk77127	vEdge 2000 Temperature Sensors Board failed after upgrade to 18.3
CSCvk77901	Policy attach preview fails on vSmart after upgrading from 17.2.x to 18.3.0
CSCvk77926	seeing device off-line for a vEdge on a template push even when it has control up/up
CSCvk78034	Multiple VRRP groups sending exact same VRRP advertisement causing VRRP split brain in 18.3.0
CSCvk78896	ompd crash
CSCvk79264	tcpd core on vedge5k upon reloading with traffic
CSCvm15501	Evaluation of vedge for CVE-2018-5391 (FragmentSmack)
CSCvm46846	PS1 flapping - Logs reporting "Power supply '1' down or not present" the power supply is then report
CSCvm47232	Ping from host to the virtual IP is failing when VRRP failover is executed twice.
CSCvm49076	svi feature template missing for C1117-4P models.
CSCvm51340	Template push fails because of '&' in interface description
CSCvm51612	Cloud onRamp: Upgrading a 17.2 setup with COR elements to 18.3+ is broken
CSCvm53094	DHCP server configs are not getting mapped for cedge if excluded address is not filled in
CSCvm53683	vManage shouldn't generate "ip vrf forwarding 0" configuration for TACACs in global table for cEdge
CSCvm53853	On push of a vSmart-data-policy w/ cflowd as accept causes vEdge(s) to crash with
CSCvm57114	' logging source-interface "" ' created by vManage when enabling syslog
CSCvm57126	Incorrect VRF name mapping for syslog source VPN in vManage

Caveat ID Number	Description
CSCvm60099	Handling of O field and Enterprise Root CA with vEdge-Cloud is resulting in vEdge-Cloud bringup fail
CSCvm64908	vManage creates invalid interface with incorrect VLAN interface format
CSCvm65707	vManage: TLOC-Extension configuration is not generated for cEdge
CSCvm68185	Instance of Cloud onRamp was deleted/Not migrated when update 17.2.8 to 18.3.1

Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.2a and Cisco SD-WAN Release 18.3.2

Table 10: Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.2a and Cisco SD-WAN Release 18.3.2

Caveat ID Number	Description
CSCvi24304	IOSD core on: applying qos service-policy on interface X and running 'duplex' oper on interface Y
CSCvk77731	I/O Errors on c5.4xlarge - vManage/vBond/vSmart
CSCvm46846	PS1 flapping - Logs reporting "Power supply '1' down or not present" the power supply is then report
CSCvm61043	ISR4331 crash seen with traffic and app router policies at Loblaw
CSCvm64768	CoR: Expand limit of VPN Numbers for mapping

Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.2 and Cisco SD-WAN Release 18.3.1.1

Table 11: Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.2 and Cisco SD-WAN Release 18.3.1.1

Caveat ID Number	Description
CSCvk77731	I/O Errors on c5.4xlarge - vManage/vBond/vSmart
CSCvm49076	svi feature template missing for C1117-4P models.

Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.2 and Cisco SD-WAN Release 18.3.1

Table 12: Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.2 and Cisco SD-WAN Release 18.3.1

Caveat ID Number	Description
CSCvi56366	CRL Key Usage Checking Issue
CSCvi59800	port mirroring for inbound traffic flows fails when changing network addressing without removing acl
CSCvj90245	vtracker crash interface after link bounces
CSCvj94133	ASR1001-X : netconf interface goes into oper down state afer reboot tests

Caveat ID Number	Description
CSCvk21245	vEdge NAT: 2 different source-private-ips mapped to same source-pub-ip + source-pub-port. Tloc exten
CSCvk23108	SVM: template node missing edge
CSCvk27018	cEdge policy: Policy download to dp failed with app-list in data policy
CSCvk27394	cEdge need to read day0 bootstrap files from cdrom
CSCvk27736	Cellular controller yang models not included for ISRv
CSCvk31172	Need an exception to not check for site id when the devices are in staging during upgrade
CSCvk33230	NAT translation is not working on ASR1002-HX
CSCvk34720	vlan interface ip continue to advertise even though no physical interfaces associated
CSCvk36354	WWAN : Support to configure user name/pass on AT&T firmware
CSCvk38490	OMP daemon crash on vSmart running 17.2.6
CSCvk38707	Cellular - Last Resort : IP address is retained and LR interface comes UP when primary is stable
CSCvk38993	vEdge NAT: Regular NAT interface on vEdge shows inconsistent behavior, once its private-to-public po
CSCvk45960	Alarms not being populated in the vManage GUI
CSCvk50773	Template attach failed with error: Vty line 0 doesn't exist
CSCvk54504	18.2.0 to 18.3.0 code upgrade fails on vmanage
CSCvk56456	unable to add 3rd device to cluster in 18.3.0
CSCvk64590	VRRP unable to reach the virtual ip
CSCvk77283	Cannot set the main-interface/sub-interface mtu greater than 1500/1496

Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.2 and Cisco SD-WAN Release 18.3.0

Table 13: Resolved bugs in Cisco IOS XE SD-WAN Release 16.9.2 and Cisco SD-WAN Release 18.3.0

Caveat ID Number	Description
CSCvj60148	cedge_policy: policy counters are not getting updated after changing the counter name.
CSCvj92237	cEdge ospf password: On changing the ospf password, the commit fails
CSCvj98370	vdaemon cash on TSN OPENSSL_cleanse

Caveat ID Number	Description
CSCvk21130	If device is decommissioned from vmanage then request platform software sdwan config reset is throw
CSCvk36514	realtime for zonepair sessions for vedge is throwing error in vmanage.

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 16.9.2 through 16.9.6 and Cisco SD-WAN Release 18.3.0 through 18.3.8.

Bug ID	Description
CSCuy24258	Bulk sync failure with "bgp ha-mode sso prefer"
CSCvf27566	OpenDNS local-domain bypass on ISR4k stop working after reboot
CSCvh22300	Update IOS XE OSPFv2 ELL private TLVs to IANA codepoints
CSCvh94044	cedge_policy: datapolicy with no seq default drop is not working from-service
CSCvi32788	Invalid error message when a vsmart policy push fails
CSCvi34649	In the AAA feature template, for radius, the secret key doesn't work even though the same for CLI wo
CSCvi35220	On headend device, enabling DPI was making the traffic entering LLQ - q0 very bursty
CSCvi37645	snmp interface description is limited to 32 characters
CSCvi42655	vManage-cEdge: Unable to reset interface through UI
CSCvi43327	After silent reboot vmanage was out of sync with cluster
CSCvi45659	Stale BFD sessions resulted in a route absence for the traffic
CSCvi46383	tabulation doesn't work with ping command
CSCvi49913	last resort should not be activated when omp is in init or down state
CSCvi54347	vSmart policy has been pushed to the devices but was not applied
CSCvi59620	Unable to adjust MTU on interfaces that are part of a bridge interface
CSCvi59626	Routes are being incorrectly installed in the routing table even though there is no bfd b/w the vEdg
CSCvi59799	Default Management VPN incorrectly named "Transport VPN"
CSCvi66931	Small packet loss seen when switching traffic from biz-internet tunnel to LTE
CSCvi80775	Decouple buffer allocation for egress queues from the interface speed negotiated

Bug ID	Description
CSCvi88112	LFTS2.0: lsmpi-rx/4029/0x00000300 backtrace when control connections are coming up on cedge-TSN
CSCvi97773	vmanage_zbfw: one vpn should not be configured as part of more than one zone.
CSCvj00848	Cluster failover: If NMS services are down on one of the vManage, UI is stuck while performing any o
CSCvj17396	Feature Template: BGP neighbor route-policy variable name shows as default value in feature policy t
CSCvj29075	vManage-MTT-Cluster-Failover: Double failover of leader results in database issue
CSCvj29165	ENH - all user groups for cEdge are configured with same privilege 15
CSCvj32215	hostnames that use a "." period will not fully display use a _ or - to workaround
CSCvj38580	MT Cluster Failover: Cluster got into a bad shape when one vManage node was rebooted while vEdge ima
CSCvj41271	localized policy- Qos Map: Queue shows classmap field as blank if user has deleted the class map fro
CSCvj43085	Cannot change accept or drop in VPN Membership
CSCvj43195	admin-tech enhancement for ATM/Dialer information
CSCvj50058	The vManage DPI screen displays a DIA graph for a vEdge router on which local Internet exit is not c
CSCvj54679	admin-tech enhancement for DSL debugs
CSCvj58797	17.2.5 and seeing a bug similar to VIP-8344 - gzip consuming lots of CPU
CSCvj67940	show omp tlocs advertised is not filtering correctly to the TLOC adv. routes
CSCvj79456	GUI of vManage running 17.1.3 was not opening, seeing exceptions in vmanage-server.log
CSCvj82776	Incorrect tag for omp routes
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
CSCvj94072	AWS Instance Type Change from C3 to C4 Fails
CSCvj95656	Some of the eem options are missing under confd
CSCvk08395	Cellular profile not being written to the Modem
CSCvk10038	vedge-cloud activate does not give feedback when no organization name is configured

Bug ID	Description
CSCvk11112	User may hit issue that packet capture failed at "Device Error: Failed to read server configuration"
CSCvk12352	Config Diff is not lining up properly
CSCvk15467	Optional parameters in template breaks XML stream towards devices
CSCvk16663	Static IP configured on transport interface during PnP workflow
CSCvk23051	messaging server ends up in bad state
CSCvk27129	The requirement to shutdown Dialer interface before its deletion causes an issue for vManage
CSCvk27232	Controller deletion from vManage should be ignored by device
CSCvk27493	Sync up data stream configuration and provide a way to force the sync
CSCvk29013	CPU utilization is seeing an upward trend on the vEdge 2000 and vEdge 1000 nodes
CSCvk29514	removing dsl config from vmanage fails.
CSCvk31357	Application communication failure on the vSmart
CSCvk32990	ST and MTT ZTP failure - Failed to process install action: java.lang.NullPointerExceptio
CSCvk33216	Handle ZTP constraint for MTT setup after upgrade
CSCvk34856	cEdge: vpn 0 traffic is not nat'ed over tloc-extension interfaces
CSCvk36517	zbfw_vmanage_cedge: zonepair statistics entries are not consistent with device.
CSCvk38122	SSH terminal not working in multitenant vManage mode
CSCvk40360	SVM: ZTP install causes a SW install task to fail
CSCvk40435	CVM: deleting vManage instance from a cluster fails
CSCvk40521	WRR scheduler favoring queues with large packets
CSCvk44405	Control connection fail to come on interface with NAT and ACL with default-action drop
CSCvk44649	Upgrade from 18.2.0 to 18.3.0 was failing
CSCvk52771	Throughput degradation noticed on vEgde100 with IPv6 Underlay
CSCvk53396	NCS entries are missing after upgrading the vManage from 17.2.6 to 18.3.0
CSCvk56629	Unable to reboot the device, and upgrade-confirm changes active to False.
CSCvk57214	vManage fails to generate CSR

Bug ID	Description
CSCvk58084	Not all email alerts are getting generated consistency
CSCvk59440	Update default timers for control
CSCvk61571	Unable to ssh from vedge to vmanage
CSCvk63612	[some] vEdges became unreachable up on vEdge-List push from vManage
CSCvk65125	Template migration failed while upgrading from 17.2 to 18.2. (BEMS839161 Case: 00015295)
CSCvk65202	cEdge GPS location is not updated through vManage feature template
CSCvk67084	when we use UUID in upper case to activate vedge cloud, device-life cycle is not going through.
CSCvk69670	vManage failed to activate 18.3.0 from 18.2.0
CSCvk72673	SVM: Cflowd should be removed from statistics settings
CSCvk72903	cEdge-vDaemon: Sub-interface's control-local-properties shows state=UP even though it is admin-down
CSCvk72985	Device goes out-of-sync during network flap and never attempts template push after it is reachable
CSCvk73077	Not able to push the templates
CSCvk76181	vmanage localized policy ACL when matching ports syntax issues
CSCvk77142	DF bit is being set on cflowd template packets
CSCvk77198	General Motors - 16671- after upgrade to 18.3.0 from 17.2.7 - vManage is reporting all vEdge 2000's
CSCvk77234	vmanage no longer accepts "/" character in variable naming
CSCvk77270	CLONE - On headend device, enabling DPI was making the traffic entering LLQ - q0 very bursty
CSCvk77480	An '&' character in the organization-names breaks template pushes
CSCvk77546	Added sub-int in VPN 0 does not appear in "show interface" output
CSCvk77696	vEdge 100M Cellular VPN interface template can't be saved
CSCvk77988	Cannot copy built-in App List Google_Apps and Microsoft_Apps
CSCvk77997	Azure vEdge Cloud Public IP bound to management NIC
CSCvk77999	Unable to instantiate new Azure vEdge Cloud on existing Resource Group
CSCvk78100	Can't push vSmart policy because vManage thinks it is offline, but reachable

Bug ID	Description
CSCvk78273	An "&" in org-name/sp-org name causes CSR failure for vEdge cloud
CSCvk78335	OSPF NSSA prefixes (N1, N2) are not advertised into OMP
CSCvk78359	vEdge Crashed when issuing a "show ospf ... " command
CSCvk78638	Packet drop observed on Finisar FCLF8521P2BTL SFP when speed changed from 1000 to 100.
CSCvk78682	vEdge 1K silent reboot with reboot reason Soft Reset(Watchdog)
CSCvk79079	SSO Requires browser cache to sign in after first login
CSCvk79267	SVM: vbond cannot be upgraded
CSCvk79278	2 software forced reloads with 18.3.0 on vEDGE-100m
CSCvk79322	vEdge 5000 router rebooted multiple times. Error message : Software initiated FP core Watch dog fail
CSCvm01519	Intermittent HMAC errors seen on TSN for ASR 1001-HX BFD sessions
CSCvm26371	cEdge ISR4331: CPP Ucode Crash seen on multiple ISRs when LR condition is being removed
CSCvm26391	ECMP is not working in some scenarios
CSCvm37501	linux_iosd crash and router reload when un-configuring md5 on ospf interface
CSCvm38184	Duplicate device entry created when activating vedge cloud chassis-id that is generated on PnP
CSCvm39500	Drops not showing up in show interface queue
CSCvm40434	Interface is not getting programmed in VPN 0 when we move from Auto IP to static IP address assignme
CSCvm40554	DPI summary stats show no active flows incorrectly after switching in-n-out of OOM
CSCvm42410	Device status on GUI configuration -> templates shows device status Out of Sync
CSCvm42884	vEdge100m Crash when workstation requests DHCP adress
CSCvm46901	upgrading from 16.2.10 to version 17.2.7 and internal script is failing during the upgrade /usr/bin
CSCvm46954	vEdge 5K Template Attach - Null Error Msg
CSCvm48892	Missing flow-sampling-interval in SNMP query
CSCvm49899	ve100m throughput drop when QOS config is applied
CSCvm55390	template push with static default not getting pushed until it is manually toggled

Bug ID	Description
CSCvm57183	Enabling cloud-qos on VE5K drops forwarding performance significantly less than 1.5M pps
CSCvm59347	Activating Simply control policy causes 1of2 vsmarts to reboot
CSCvm60350	OBS: cannot delete bfd from interface via netconf
CSCvm60561	loss latency jitter not being calculated on cEdge
CSCvm60731	5k performance degradation between 18.3.0 and 18.3.1
CSCvm62262	SD-WAN 18.3.1: 'Device Monitoring' privelege does not give access to 'Monitor-Georgraphy' in GUI
CSCvm62440	Connection refused for template push, device is online
CSCvm62586	vEdge 5000 control connections are not coming up after a reboot.
CSCvm63759	"no exec" is pushed as part of console configs in a cedge tempate on 18.3.1 cuts off console access
CSCvm68056	Incorrect VRF name mapping for NTP source VPN in vManage
CSCvm68397	NTP source interface configuration is not genrated by vManage
CSCvm70027	GC allocations errors causing GUI to be unresponsive
CSCvn38487	vManage does not generate proper AAA configuration for Cisco XE SD-WAN Router
CSCvq67476	ikev2 dpd retransmit always 1s and fails after one retry with "giving up after 1 retransmits"
CSCvm42581	ftmd crash while changing rewrite rule PLP from high to low
CSCvp44731	Unable to ping to the virtual gateway IP when VRRP is configured on 10G sub-interfaces on vEdge5K

- If you configure IPv6 on a cellular interface, the control connections might go down and come back up continuously. [VIP-21970]
- When two routes exist to the same neighbor, if you specify a single IP address in the show ip routes command, the command might return only one of the routes, but if you specify an IPv4 prefix and prefix length, the command returns both routes. [VIP-32736]
- For IEEE 802.1X, you cannot configure a RADIUS server for MAC authentication bypass (MAB). [VIP-18492]
- In application-aware routing policy, the salesforce_chatter, oracle_rac, and google_photos applications might not be classified properly. [VIP-21866]
- If you misconfigure the target VPN for NAT, the ICMP unreachable messages might contain the inside IP address. [VIP-43947]

- When forwarded ports are not open on the inside client, NAT might block RST packets in the return path and might generate ones on behalf of outside client. [VIP-43950]
- You might not be able to configure the Cloud Onramp VPC even when vEdge routers are present. [VIP-34655]
- In vManage NMS, when you use the policy configuration wizard to create policies for a mesh topology, you might need to create an additional policy using a CLI template for the mesh policy to work. This situation is known to occur in a network that has two regions, where each region is mesh that is a subset of the entire network, where each region has its own data center, and where the branch vEdge routers in one region communicate with branch routers in the other region through the data centers. We will call these Region 1 and Region 2. Assume that Region 1 has a control policy that advertises its TLOCs to the data center in Region 2, and Region 2 has a control policy that prevents the spokes and data center in Region 2 from advertising TLOCs to the spokes in Region 1. The result is that the data center in Region 2 repeatedly attempts to form control tunnels to the data center in Region 1, but these attempts fail. As a workaround, you must a policy using a CLI template that allows the data center in Region 2 to exchange TLOCs with the data center in Region 1 and then attach that policy to the vEdge routers. [VIP-29933]
- In an overlay network with three vSmart controllers, if a controller group list configured on a 100 vEdge router contains two vSmart controllers, the maximum number of controllers that the router can connect to is set to two, and the maximum number of OMP sessions on the router is set to two, 50 routers connect to each of two vSmart controllers. If you bring these two controllers down, all 100 connections then move to the third vSmart controller. However, if you then bring up one of the other vSmart controllers, 50 connections move to that controller, but the third controller might still have 100 connections. [VIP-27955]
- When a certificate for controllers is about to expire, no syslog message is generated. [VIP-28960]
- On vEdge routers, when you issue an nping command for IPv6, the command might fail, and a core file might be created on the router. From vManage NMS, you issue this command from the **Monitor** > **Network** > **Troubleshooting** > **Ping pane**. From the CLI, you use the tools nping command, specifying options "--ipv6". [VIP-31924]
- On a vEdge 100m router, after you execute the request software reset command, the router might reboot continuously. [VIP-24149]
- If you try to configure a vEdge router using vManage configuration templates, you might see errors related to lock-denied problems. As a workaround, reboot the router. [VIP-23826]
- You might not be able to edit configuration templates, with the vManage server reporting that multiple users are trying to edit the template at the same time. [VIP-27615]
- When you use the vManage NMS and the CLI show system status command, the reboot reason is incorrect; it is shown as unknown. The /var/log/tmplog/vdebug logs shows that the system reboot happened because of a user-initiated upgrade to Release 17.1.3. [VIP-31222]
- You might not be able to push configuration templates to vEdge routers. [VIP-34886]

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 devices with the SFP-10G-SR module do not support online insertion and removal (OIR) of this module.

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 software 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.
- VRRP on vedge-cloud is not supported on ESXi x86 devices due to ESXi limitations. On vmxnet3, an error message will be thrown while attempting to configure VRRP. On E1000, error message will not be thrown, but VRRP will not function as configured.

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 Viptela 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 Viptela 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.

IPsec

- For IKE-enabled IPsec tunnels that use IKE Version 2, the SD-WAN software does not support Traffic Flow Confidentiality (TFC) padding for ESP Version 3, as defined in RFC 4303, IP Encapsulating Security Payload (ESP).

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 Viptela controllers 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.
- 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.

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. Viptela 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 Viptela 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 Viptela 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 Viptela 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 $4 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.
- Once 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.
- Base licensing package of AX needs to be enabled for IOS-XE SDWAN ISRv during VM deployment on the ENCS portal.

YANG Files for Netconf and Enterprise MIB Files

Netconf uses YANG files to install, manipulate, and delete device configurations, and Cisco vEdge device supports a number of enterprise MIBs.