Release Notes for Cisco IOS XE Catalyst SD-WAN Release 16.11.x and Cisco SD-WAN Release 19.1.x

First Published: 2019-04-15

Release Notes for Cisco IOS XE SD-WAN Release 16.11.x and Cisco SD-WAN Release 19.1.x

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

These release notes accompany the Cisco IOS XE SD-WAN Software Release 16.11, which provides Cisco SD-WAN capabilities for Cisco IOS XE SD-WAN routers, and the compatible Cisco SD-WAN Software Release 19.1 for Cisco SD-WAN controller devices—including vSmart controllers, vBond orchestrators, vManage NMS, and vEdge routers.

Supported Devices

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

New and Enhanced Software Features

New Features

- Additional DHCP options–This release adds support for vEdge routers for DCHP server options 43 and 191, which you can use when you configure the IP addresses of a default gateway, DNS server, and TFTP server in the service-side network and the network mask of the service-side network.
- Advanced Malware Protection (AMP) integration–Equips SD-WAN platforms to provide protection and visibility through stages of the malware lifecycle, before, during, and after.
- Cisco PKI support for SD-WAN controllers–Support for migration from Symantec certificates to Cisco-signed certificates.
- CLI template support–This release support the use of a CLI template for deploying IOS-XE SD-WAN routers.

- Cloud onRamp Auto-scale support for AWS–This feature provides an AWS Transit-VPC architecture that allows the dynamic discovery of all of the applications (host VPCs) that are running in any specific region of an AWS and create a transit VPC with vEdge Cloud and then map the application to specific VPN segments.
- Cloud OnRamp configuration for IaaS–Extends the fabric of the Cisco SD-WAN overlay network into public clouds by creating Cloud vEdges or Cisco Cloud Services Routers (CSRs), which provide the connectivity to cloud applications that customers host on these public clouds.
- Container reload and reboot–The container reload feature lets you re-install a snort container image, and the container reboot feature lets you stop and then start a snort container.
- Custom packaging for Cloud onRamp for CoLocation–You can now edit VM packages to update default configuration items.
- Customizable service chain for Cloud onRamp for CoLocation–You can now create a customizable service chain with day0 configurations.
- Forward-directed broadcast packets–You can configure forwarding of IP-directed broadcast packets for vEdge routers on selected LAN interfaces.
- Forward error correction–You can configure forward error correction (FEC) on IOS-XE SD-WAN routers, which provides for the recovery of lost packets on a link by sending extra “parity” packets for every group (N) of packets.
- IPv6 for transport–This release supports the configuration of IPv6 for Gigabit Ethernet on IOS-XE SD-WAN routers, PPPoA, PPPoE, IPoE, Cellular, Multilink, and T1/E1 interfaces.
- ISR 4461–This release adds support for the Cisco ISR 4461, a new member of the Cisco 4000 Integrated Services Router series.
- Micro-tenancy RBAC by VPN–You can create sub-tenants for a tenant, based on a VPN or groups of VPNs. A device at a site can be configured with multiple sub-tenants (VPNs).
- NAT64–This release supports NAT64 to facilitate communication between IPv4 and IPv6 IOS-XE SD-WAN routers.
- Serial file allowed list validation–Provides validation of a device serial file that vManage sends to vBond or vSmart to ensure that the file has not been tampered with.
- Standard IPSEC support–This release provides support for standard IPSEC (IKEv1/IKEv2) tunnels over a service VPN for IOS-XE SD-WAN routers.
- Support for enterprise certificates–vEdge and IOS-XE-SD-WAN routers support enterprise certificates for device verification.
- Support for EIGRP–This release adds support for Enhanced Interior Gateway Routing Protocol (EIGRP) on the service side for IPv4 for IOS-XE SD-WAN routers.
- SWIM support for all devices in a Cloud onRamp for CoLocation cluster–vManage provides image management for an entire Cloud onRamp for CoLocation cluster.

New and Enhanced Hardware Features

New Features

- Support for ISR 4461: The Cisco IOS XE SD-WAN software runs on ISR 4461 from IOS XE SD-WAN Release 16.11

Important Notes, Known Behavior, and Workarounds

- Devices operating with Cisco SD-WAN XE 16.11.1a cannot be downgraded to 16.10.4.
- Use of port-channels on the Service Side VPN is not supported on Cisco IOS XE Catalyst SD-WAN devices.
- Bridge Domain Interface (BDI) is not supported on the Cisco ASR1000.

Resolved and Open Bugs

About the Cisco Bug Search Tool

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

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

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

Resolved Bugs

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

Bug ID	Description
CSCvj29165	ENH - all user groups for cEdge are configured with same privilege 15
CSCvj84204	cEdge: Control connections fail if DNS server is not reachable thru one TLOC interface in ECMP
CSCvk27129	The requirement to shutdown Dialer interface before its deletion causes an issue for vManage
CSCvn10158	Not able to restart config-db after cleaning up disk space issue under /opt/data
CSCvn22546	vManage needs to adjust memory threshold for warnings on cEdge platform
CSCvn44400	Login banner does not take me to next line when I give '\n' for cEdge devices.
CSCvn59626	NTP template attach fails with a non default vrf and source interface configured
CSCvn63395	ASR-1002-HX crash at headend running 16.9.3
CSCvn67591	Timeout Seen When Previewing Policy Using UI Policy Builder

Bug ID	Description
CSCvn71621	ping and traceroute functionality to bypass routing and specify next-hop for SDWAN fabric tshoot
CSCvn97821	monitor/network/wan/tunnel - real time table columns are reverse selection
CSCvo00790	cedge_cli_template: Unable to move interface from global vpn
CSCvo06805	No fallback to datacenter when INET link is down
CSCvo21464	MIPS images writing a bunch of FP printf() output to main console
CSCvo32377	Adjust NAT timeout values in vManage templates for cEdge
CSCvo33693	vEdge-1000 using DIA and ZBFW having issues intermittenly with iframes of specific site after zbfw s
CSCvo40967	linux_iosd memory goes up on ISR1100 over extended soak
CSCvo43917	SPF type5 LSA might not be flushed with overlapping prefixes
CSCvo46350	allow service SNMP in the Tunnel properties in VPN Interface template
CSCvo65825	omp route tag shown up incorrectly in IOS rib database
CSCvo69320	ISR ipv6/dhcp tloc got DCONFAIL failure when connecting to vbond
CSCvo78034	vpn 65538 [umbrella] missing when upgrading from 16.9 to 16.11
CSCvo88612	Fixing Renewal/Revocation of enterprise certs on cEdge- follow up commit of CSCvo36029

Open Bugs

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

Bug ID	Description
CSCvn94117	Deleting a segment on network builder doesn't delete the segment completely
CSCvo12826	Setting "Collect admin-tech on reboot" to On in System Feature template does not work for cedge
CSCvo13180	cEdge VRF ID changes removes the VRRP virtual IP from IOSD and not from confd
CSCvo26830	workaround for failure to update ikev1 to ikev2 config from vmanage.
CSCvo40410	vManage-UTD: In security dashboard, issues in displaying signature names
CSCvo46253	BGP Oper model rpc reply error with aggregate bgp ipv6 route.
CSCvo54319	MT Cluster: Failed to commit Kafka Error seen on one of the vManage during any device operation

Bug ID	Description
CSCvo60482	Unable to generate config preview if secondary IP add is added when primary is dynamic
CSCvo62587	Need next hop use interface together with address as option for the ipv6 static route
CSCvo67056	Template push is failing with max character (2048) values for banner template
CSCvo67128	Enabling/Disabling overlay-as under omp causes service BGP route to be removed from omp.
CSCvo73934	Redistribute bgp and ospf with route policy from Eigrp template fails to attach to the cEdge device
CSCvo79398	XE router crashed while un-configuring vrf vpn configuration
CSCvo88482	Unable to attach ipv6 acl to SVI interface which is used under transport VPN
CSCvo89232	Unable to support default value for VRRP timer on VPN interface Ethernet template
CSCvo91255	cEdge ISRv Certificate installation is failing with RPC error
CSCvo92352	vEdge x86 and mips file sizes have grown almost double from 18.4 branch to 19.1 branch
CSCvp00165	OSPF Feature Template : Area nssa summary and translate not configured on CSR
CSCvp00254	Control Node down , Control Site Down Alarms missing on graceful shutdown of transport interfaces
CSCvp11416	cEdge - Template attach fails for a cedge device if theres a central policy with cflowd activated
CSCvp12510	TAIL-F: Passwords more than 32 characters in length fail when doing push from vManage (CSCvo93386)
CSCvp13210	Centralized Policy APIs providing incorrect results for isActivatedByVsmart and reference count
CSCvp13833	snmp-server trap-source configuration is not generated for cEdge by vManage
CSCvp15058	IPv4 Control connection flaps when WAN transport interface configured ipv6 address
CSCvp23780	Cedge-vManage-19.1 - vManage radio button for turning off Tunnel fails and throws error message
CSCvp24088	upgrade fail on ISRv with only 2 images in system due to cdb space issue
CSCvp26156	config preview fails when bandwidth & clock rate set to global on T1/E1 interface template
CSCvp31347	banner multiline tag is causing an issue with the quotes
CSCvp33693	Upper/lower case of Ipv6 address from template attach may cause device go offline

Bug ID	Description
CSCvp36072	NTP template attach is missing source interface when non default vrf and source interface configured
CSCvs83533	Vedge 1k running 19.2.1 constantly reboots with the reason "USB controller disabled or enabled"

Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations

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

ROMmon Requirements Matrix

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

Table 1: ROMmon Versions

Device	ROMmon Version for 16.10 Devices	ROMmom Version for 16.11 Devices
ASR1000-X/HX	16.3(2r)	16.3(2r)
ISR 4000	16.7(4r)	16.7(4r)
ISR 1000	16.9(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 following table.

Table 2: Minimum CIMC and NFVIS Software Versions for ISRv Routers

Hardware Platform	CIMC	NFVIS
ISRv	3.2.4	3.9.2

Related Documentation

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

© 2019–2021 Cisco Systems, Inc. All rights reserved.