Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.1.x

First Published: 2020-04-15

Last Modified: 2021-03-30

Release Notes for Cisco vEdge Device, Cisco SD-WAN Release 20.1.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 RFP documentation, or language that is used by a referenced third-party product.

These release notes accompany the Cisco SD-WAN Release 20.1.x, which provides Cisco SD-WAN capabilities. They include release-specific information for Cisco vSmart Controllers, Cisco vBond Orchestrators, Cisco vManage as applicable to Cisco vEdge devices.

For release information about Cisco IOS XE SD-WAN devices, refer to Release Notes for Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release Amsterdam 17.2.x

For release information about Cisco NFVIS SD-Branch, refer to Release Notes for Cisco NFVIS SD-Branch, NFVIS Release 4.1.1 and vManage Release 20.1.1.1

For release information about Cisco SD-WAN Cloud OnRamp for Colocation Solution, refer to Release Notes for Cisco SD-WAN Cloud OnRamp for Colocation Solution, Release 20.1.1

What's New for Cisco SD-WAN Release 20

This section applies to Cisco vEdge devices.

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

Table 1: Cisco SD-WAN Release 20.1.1

Feature	Description
Systems and Interfaces	

Feature	Description
Default Device Templates	A default device template provides basic information that you can use to bring up devices in a deployment quickly. This feature is supported on the Cisco Cloud Services Router 1000V Series, Cisco C1111-8PLTELA Integrated Services Routers, and Cisco 4331 Integrated Services Routers.
Forwarding and QoS	
Per-Tunnel QoS	This feature lets you apply a Quality of Service (QoS) policy on individual tunnels, ensuring that branch offices with smaller throughput are not overwhelmed by larger aggregation sites. This feature is only supported for hub-to-spoke network topologies.
Policies	
Device Access Policy on SNMP and SSH	This feature defines the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. The control plane of Cisco SD-WAN processes the data traffic for local services (like SSH and SNMP) from a set of sources in a VPN. Routing packets are required to form the overlay.
Support for SLA Classes	This feature allows you to configure upto a maximum of eight SLA classes on Cisco vSmart Controller. In previous releases, you could only configure upto four SLA classes. This allows for additional options to be configured in an application-aware routing policy.
Security	
Additional Cryptographic Algorithmic Support for IPSec Tunnels	This feature adds support for HMAC_SHA256, HMAC_SHA384, and HMAC_SHA512 algorithms for enhanced security.
Support for Tunneling to Secure Internet Gateways	This feature allows you to integrate your routers with a Secure Internet Gateway to perform security processing and ensure that your device's performance is not affected by processing security rules.
Manual Configuration for GRE Tunnels and IPsec Tunnels	This feature lets you manually configure a GRE tunnel by using the VPN Interface GRE template or an IPSec tunnel by using the VPN Interface IPSec template. For example, use this feature to manually configure a tunnel to a SIG.
Network Optimization and High Availability	
Monitor Cluster Activation Progress	This feature displays the cluster activation progress at each step and shows any failures that may occur during the process. The process of activating a cluster takes approximately 30 minutes or longer, and you can monitor the progress using the vManage task view window and events from the Monitoring page.
QoS on Service Chains	This feature classifies the network traffic based on the Layer 2 virtual local-area network (VLAN) identification number. The QoS policy allows you to limit the bandwidth available for each service chain by applying traffic policing on bidirectional traffic. The bidirectional traffic is the ingress side that connects Catalyst 9500-40X switches to the consumer and egress side that connects to the provider.

Feature	Description
VNF States and Color Codes	This feature allows you to determine the state of a deployed VM using color codes, which you can view on the Monitor > Network page. These color codes help you make decisions on creating service chains based on the state of the VM.
Network Utilization Charts for SR-IOV Enabled NICs and OVS Switch	This feature allows you to view network utilization charts of VM VNICs connected to both SR-IOV enabled NICs and OVS switch. These charts help you determine if the VM utilization is optimal to create service chains.
Monitor and Maintain Guide	
Enable Trace for OMP agent and SD-WAN subsystem	This feature enables monitoring and controlling the event trace function for a specified SD-WAN subsystem. Event trace provides the functionality to capture the SD-WAN traces between the SD-WAN daemons and SD-WAN subsystems.
Admin-tech Enhancements	This feature enhances admin tech file to include show tech-support memory, show policy-firewall stats platform and show sdwan confd-log netconf-trace commands in the admin-tech logs. The admin-tech tar file includes memory, platform, and operation details.

Important Notes, Known Behavior, and Workaround

When you complete a Cisco SD-WAN software downgrade procedure on a device, the device goes into the configuration mode that it was in when you last upgraded the Cisco SD-WAN software on the device. If the device is in a different configuration mode when you start the downgrade than it was when you last upgraded, the device and Cisco vManage show different configuration modes after the downgrade completes. To put the configuration modes back in sync, reattach the device to a device template. After you reattach the device, both the device and Cisco vManage show that the device is in the vManage configuration mode.

Cisco vManage Upgrade Paths

Table 2:

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

Supported Devices

Table 3: Supported Devices and Versions in Cisco SD-WAN Release 20.1.1

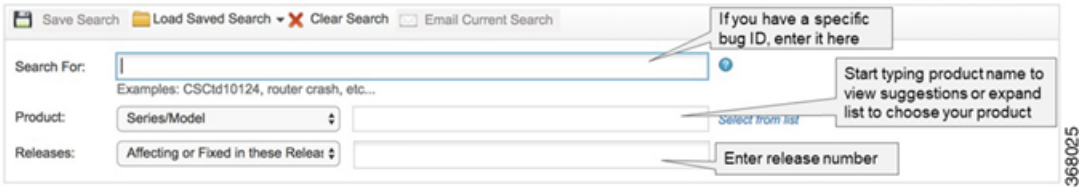
Device Family	Device Name
vEdge Routers	• vEdge 100, vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000 • ISR1100-6G/ISR1100-4G, ISR1100-4GLTENA, ISR1100-4GLTEGB

Resolved and Open Bugs

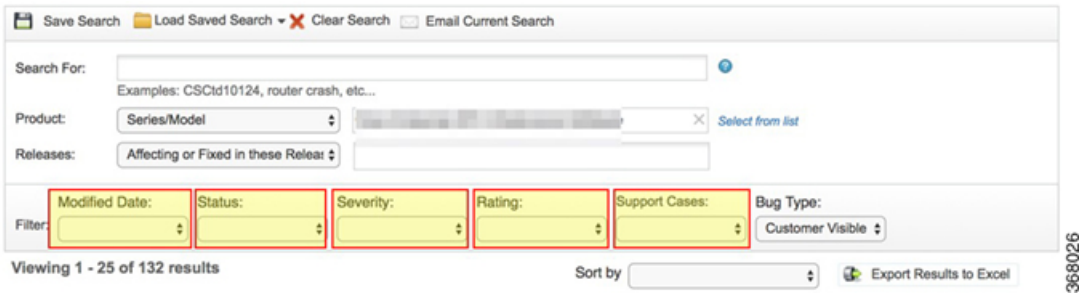
About the Cisco Bug Search Tool

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.



Bugs for Cisco SD-WAN Release 20.1.2

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

Resolved Bugs for Cisco SD-WAN Release 20.1.2

Table 4: Resolved Bugs

Bug ID	Description
CSCvk78938	Upload of a corrupted serial file can lead to DOS situation

Bug ID	Description
CSCvo72974	vE5K performance drops significantly using loopback TLOC without 'bind' configuration
CSCvq53160	vManage: SSO authentication may not be possible after upgrade/reboot
CSCvq91658	Error in sending device list for Push vSmart List to vBond
CSCvr71672	Cisco PKI Root Certificates not installed in recent images - - Polaris Side commit
CSCvs09160	Redistribution from OSPF to BGP is failing in vEdge when policy is being applied
CSCvs21315	Insecure Product Design exposes sensitive information to non-admin user
CSCvs31128	vManage - no stats for IRB interfaces
CSCvs48535	%IPSEC-3-REPLAY_ERROR: + BFD down and drops IN_CD_COPROC_ANTI_REPLAY_FAIL
CSCvs67034	vEdge1000 do not get ping reply via GUI if select source interface
CSCvs76326	SDWAN 19.2.1: IPv6 vBond not reachable/UP from vManage when DNS name
CSCvt05575	SFTP to vManage is not working after upgrade to 20.1, 19.2
CSCvt06194	DR replication time always given in PST
CSCvt15174	QoS policy is applied to both Dialer and Ethernet PPPoE WAN interface
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
CSCvt54485	Nat over IPsec not working with ZBFW
CSCvt55446	Misleading logout event
CSCvt61421	vedge-cloud with SRIOV interfaces unable to receive IP packets more than 1496 bytes
CSCvt64600	Top applications UI : Y axis (usage) not shown properly
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
CSCvt70360	Inconsistency between "show app dpi flows" output and Current flows count in show app dpi summary
CSCvt76335	vedge frequently establishing control connections to the vBond even though it is in equilibrium

Bug ID	Description
CSCvt91741	Disaster Recovery: Arbitrator causing failover every 30 minutes without any failures-Revert track
CSCvu12526	default templates can't be copied
CSCvu12536	Can't assign default router distance on sub-interface via vManage
CSCvu18159	Need to increase Smart account username character limit to more than 32 characters
CSCvu19754	Cannot ssh into vsmart, vbond with GCM ciphers
CSCvu23499	"show ip route vpn " output not showing specific routes for omp routes
CSCvu26847	isr1100 unable to communicate with vbond due to Board ID Signature Verify Failure
CSCvu29251	Unable to push localized policy to SDWAN CSR1000v deployed on cloud
CSCvu29677	vManage misleading error regarding multitenancy in singe tenant environment cluster
CSCvu31763	vEdge 5k crashing on 18.4.4 with fp-um crash files when using GRE SDWAN tunnels
CSCvu35785	Umbrella Registration Token: Not able to delete the token for Legacy devices
CSCvu41306	Need new JKS file for 19.x+ versions
CSCvu48660	Optional field is not considered as optional.
CSCvu51111	Email address including some characters cannot be entered for Email notification
CSCvu53588	DC1 vmanage template attachment disappear after a switchover
CSCvu54906	Template update :Request time out:Client timed out waiting for request taking longer than 90 secs
CSCvu55266	vEdge running 20.1 does not come up as spoke in per-tunnel QoS due to bandwidth "not set"
CSCvu55708	NCS shows down, all vbond connections fail
CSCvu57670	out of memory error on app-server wildfly
CSCvu58050	SSO SAMLResponse redirect points to loginError.html unexpectedly
CSCvu58459	Critical customer with 19.2.2, 4 vManage cluster is running into Full GC allocation failure
CSCvu59327	VManage alarms Control TLOC Down and BFD TLOC Down are not raised on the GUI all the time
CSCvu64608	vbond information is lost during replication after multiple failovers
CSCvu71611	Disable support for weak encryption ciphers on vManage and vSmart.

Bug ID	Description
CSCvu73103	vManage should prompt for new password without asking for default password if default password used
CSCvu74193	Vmanage displays error when "+:=@!'" is used in template variable
CSCvu79512	Manual Disaster Recovery: Primary vmanage is in read-only mode when secondary vmanage is down
CSCvu84389	Shared vSmart may fail to get upgraded from 20.1.1 to 20.1.12
CSCvu87254	vManage spends 60+ seconds to parse the device template with 500+ variables
CSCvu95045	Neo4j password retrieve during config-db restore is broken
CSCvu99861	Vedge end of line for the banner in 20.1 is not working as it did in 19.2
CSCvv00116	Vmanage 20.1.12 when selecting "Mark as optional" under radius will fail with an error
CSCvv03068	vEdge control connections goes down after CSR generation
CSCvv07412	Device is unreachble, interfaces are showing as up
CSCvv10287	CoR probes working for O365 but failing for every other SaaS application
CSCvv14033	vManage revokes devices enterprise cert after hitting "Send to Controllers"
CSCvv17381	vEdge5000: control connection stuck in "Challenge" phase - Failed to create IdentityReqBlob
CSCvv18311	fpmd crashes on vEdge1k, 2k with 19.2.1, 18.4.302
CSCvv19652	vEdge crashes with dbgd failed message when running speed test
CSCvv22385	vManage GUI down due to GC Allocation Failure on 19.2.3
CSCvv25817	vManage API call showed error message "Exceeded possible number of hits to the API".
CSCvv32338	Error occurred while generating inputs for device templates after adding 2 new rules to sec policy
CSCvv09807	Cisco SD-WAN Software Arbitrary File Creation Vulnerability
CSCvv21757	Cisco SD-WAN vManage Software Privilege Escalation Vulnerability
CSCvv21754	Cisco SD-WAN vManage Software Directory Traversal Vulnerability
CSCvv42376	Cisco SD-WAN Software Privilege Escalation Vulnerability
CSCvv42398	Cisco SD-WAN Software Privilege Escalation Vulnerability
CSCvu71921	Cisco SD-WAN Software Privilege Escalation Vulnerability

Bug ID	Description
CSCvv42551	Cisco SD-WAN Software Privilege Escalation Vulnerability
CSCvv42620	Cisco SD-WAN vManage Cross-Site Scripting Vulnerability
CSCvv02305	Cisco SD-WAN vManage Software XML External Entity Vulnerability
CSCvv42602	Cisco SD-WAN vManage Software Authorization Bypass Vulnerability
CSCvv03658	Cisco SD-WAN vManage Software Path Traversal Vulnerability
CSCvv21749	Cisco SD-WAN vManage Software Arbitrary File Creation Vulnerability
CSCvv42576	Cisco SD-WAN vManage Cypher Query Language Injection Vulnerability
CSCvw08529	Cisco SD-WAN vManage Cypher Query Language Injection Vulnerability

Open Bugs for Cisco SD-WAN Release 20.1.2

Table 5: Open Bugs

Bug ID	Description
CSCvt60866	vManage is sending wrong interface name in LI template for standard GRE tunnel
CSCvt84946	Cloud onRamp for IaaS on AWS: default route to null0 blackholes traffic sent to Internet
CSCvv69614	CSR's launched by basic template going "Out of Sync"
CSCvv54844	ConfigDB not updating username/password

Bugs for Cisco SD-WAN Release 20.1.12

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

Resolved Bugs for Cisco SD-WAN Release 20.1.12

Table 6: Resolved Bugs

Bug ID	Description
CSCvs23767	PPP auth type not able to select none for no password
CSCvs36978	Enforce Software Version : Device already has image error
CSCvs48327	ISR1100-4G, ISR1100-6G Fixed speed 100/10 full duplex config are not supported on RJ45 ports.
CSCvs67769	Can not create vManage user to access disaster recovery other than admin user
CSCvt24324	Ip route template admin distance not configurable

Bug ID	Description
CSCvt44269	Missing "switchport access vlan name XYZ" from cedge CLI - remove from vManage
CSCvt45042	Disaster Recovery: Arbitrator causing failover every 30 minutes without any failures
CSCvt52739	vManage (Cli Template): NAT DIA config is missing with CLI template push
CSCvt67122	vManage UI should make IKE1 pre-shared key mandatory, default value is causing template push failure
CSCvt70427	vManage Cluster: crash seen during vmanage uprade while system is going down
CSCvt71865	SNMP not working on tunnel interface and to loopback interface in vpn 0.
CSCvt74726	CDP true/false mapping is missing from the config preview .
CSCvt76546	"no ip redirects" is not applied to sub interface or Loopback interface during intf template attach
CSCvt80066	When a failed vBond recovers after vManages recover the vBond does not move to new active
CSCvt84696	Vmanage does not generate and push "aaa authentication dot1x" 802.1x command in cli template
CSCvt97764	Dhcp helper option not available in static mode in feature template for vedge and xe-sdwan
CSCvu06044	Per Tenant Backup Export Failed on multi tenant vManage
CSCvu10411	vmanage dr standby cluster not replicating feature templates even config-db replication is success
CSCvu19244	Edited Description field is not updated when template copy option is used
CSCvu19408	previously shared feature template cannot be edited post upgrade to 20.1
CSCvu26847	isr1100 unable to communicate with vbond due to Board ID Signature Verify Failure
CSCvu41152	Secondary vmanages not able to shutdown tunnel interface when in config template before failover
CSCvt31704	Device attached to Integration Management page on vmanage does not show up on DNA-C
CSCvu58508	CSR service vpn dropdown on Azure CSR
CSCvs99259	Cisco SD-WAN vManage SQL Injection Vulnerabilities

Open Bugs for Cisco SD-WAN Release 20.1.12

Caveat ID Number	Description
CSCvt70937	tcpd crash seen while running system-test regression

Caveat ID Number	Description
CSCvu23685	tcpd crash seen while running system-test regression
CSCvu64608	vbond information is lost during replication after multiple failovers
CSCvu53588	DC1 vmanage template attachment disappears after a switchover
CSCvo72974	vE5K performance drops significantly using loopback TLOC without 'bind' configuration
CSCvu69401	admin tech request prints some back end commands in vManage 20.1.924-56
CSCvu69388	admin tech logs some back end path in vEdge 20.1.924-54
CSCvu46440	Vmanage cluster sync failed message seen "Restart of wildfly timed out "
CSCvu51140	C5 - Device bootstrap template is not attached for vEdge-Cloud deployed on AWS using cloud init

Bugs for Cisco SD-WAN Release 20.1.1

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

Resolved Bugs for Cisco SD-WAN Release 20.1.1

Table 7: Resolved Bugs

Bug ID	Description
CSCvo69041	SVM: server config file is empty
CSCvp87702	Unable to see class-map configs on the cedge/vEdge device if used in only QoS map
CSCvq01445	Missing mapping for vrrp timer under vpn interface ethernet template
CSCvq92196	Cannot use bootstrap configuration with URL-F block page content requires SU access to remove
CSCvr13572	vManage web server fails after SSO SAML buildup
CSCvr88029	Unable to create a template for vEdge with loopback interface number greater than 1000 with tunnel
CSCvr92772	cedge stuck in "Sync Pending - Control connection UP after ZTP" on vmanage
CSCvs02513	vManage should not push "media-type rj45" when user configures speed or duplex
CSCvs08597	Template update pushing wrong interface with UTD NAT statement on Dialer interface
CSCvs40803	vmanage should push "no config-exchange request" via ipsec template for zscalar (cedge template)
CSCvs47117	Cisco SD-WAN Software Buffer Overflow Vulnerability

Bug ID	Description
CSCvs49495	CLI template push fails on vEdge if it contains special character "&" in the template
CSCvs56131	vSmart hosted on vContainer - Software install fails
CSCvs63098	No TLOC color options present in template post upgrade to 19.3.0
CSCvs64250	regression: can't configure dhcp default route in vManage 19.3.0
CSCvs68860	vManage templates are NOT available on the Secondary cluster.
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
CSCvs80421	16.12.3 ZBFW:When attached policy is deleted & new policy created, old policy still shows on vmanage
CSCvs91182	vManage is pushing additional slash '\' with the banner line breaker
CSCvs93379	vManage config preview is timing out on large config.
CSCvs93533	multi-tenant vmanage install UTD LXC failed via security policy through templates at tenant level
CSCvs96613	redistribution from ospf to bgp in vpn 0 is not mapped
CSCvs97152	Cannot make TACACs group interface device specific
CSCvt23547	Huge FW config (20k lines) ZBFW:Template push fails with message "Waiting for device response"
CSCvt28482	vedge SRIOV networks are unreachable after remote interface flap
CSCvq53168	Signature Update Failed after container upgrade/template push
CSCvr98758	vmanage performance slowdown with large configuration (acl's)
CSCvs07489	vmanage application timeout while pushing template to ISR1K with large number of ZBFW policy
CSCvs14659	Bring down ge0/0 is not causing ipsec interface to report down
CSCvs56652	SD-WAN router may delete newly created SA in a specific case
CSCvt00189	UT:basic template push failing for DUT on omp- while creating preview.
CSCvt12304	vManage cluster activate gets stuck in scheduled state
CSCvt16691	Cedge : advertise ipv6 lisp, eigrp and isis should be default to off in OMP template
CSCvt43609	Variables in CLI Add-On do not get populated on variable preview pop up
CSCvt73140	CLI Device template: Config Preview fails with server error

Bug ID	Description
CSCvt62068	SSL proxy: upload certificate is not working with enterprise as CA
CSCvi59726	Cisco SD-WAN vManage SQL Injection Vulnerabilities
CSCvi69962	Cisco SD-WAN Information Disclosure Vulnerability
CSCvk28549	Cisco SD-WAN vManage Software Path Traversal Vulnerability
CSCvk28609	Cisco SD-WAN vManage SQL Injection Vulnerabilities
CSCvk28656	Cisco SD-WAN vManage SQL Injection Vulnerabilities
CSCvk28667	Cisco SD-WAN vManage SQL Injection Vulnerabilities
CSCvs11276	Cisco SD-WAN vManage Information Disclosure Vulnerability
CSCvi59632	Cisco SD-WAN vManage Software Path Traversal Vulnerability

Open Bugs for Cisco SD-WAN Release 20.1.1

Table 8: Open Bugs

Bug ID	Description
CSCvr87762	MTCVM: tasks icon does not report a task in progress
CSCvs68870	Deleting vManage Disaster Recovery should not remove the software image from the software repository
CSCvs75048	vManage not cleared control connections alarm
CSCvs81621	vEdge changes the source address on the radius calls
CSCvt06013	QoS map can't be assigned to sub-interface without Shaping rate - hit error
CSCvt11206	vManage doesn't show number of CPU allocated in CLI and GUI
CSCvt32349	Notification not present while entering inappropriate information in ipsec int under ipsec route
CSCvt38373	vManage periodic cfgmgr crash
CSCvt50756	Doing "simulate flows" from vManage running 20.1 causes FTMD crash on ASR1002-HX running 16.12.01e
CSCvt66738	Eye icon in vManage password field disappears during next login when provided with wrong password
CSCvt68703	Page gets refreshed when a user tries to login to vManage UI after changing the user password
CSCvs97179	VEDGE 100M VZ LTE last resort circuit came UP randomly

Bug ID	Description
CSCvt05388	[vManage-UI] Password unmasking icon is not working
CSCvt31704	Device attached to Integration Management page on vmanage does not show up on DNA-C
CSCvt33046	Resume Disaster Recovery not working after upgrade
CSCvt44269	Missing "switchport access vlan name XYZ" from cedge CLI - remove from vManage
CSCvt52689	LLDP global settings feature template has no effect
CSCvt61517	ip nat inside source list nat-dia-vpn-hop-access is not being pushed down from vmanage to cedge
CSCvt63659	After attaching a device to partner, notifications not seen for serverlongpollevent
CSCvt65578	NAT field is missing the device specific option in 20.1
CSCvt67122	vManage UI should make IKE1 pre-shared key mandatory, default value is causing template push failure
CSCvt70427	vManage Cluster: crash seen during vmanage uprade while system is going down
CSCvt74726	CDP true/false mapping is missing from the config preview .
CSCvt76546	"no ip redirects" is not applied to sub interface or Loopback interface during intf template attach
CSCvt76564	'Cisco Logging' template under Disk section is missing the Priority option
CSCvs83533	Vedge 1k running 19.2.1 constantly reboots with the reason "USB controller disabled or enabled"
CSCvq53160	vManage: SSO authentication may not be possible after upgrade/reboot
CSCvv42937	No date and time info in the syslog payload
CSCvw35025	vEdge system buffer pool depletion and data plane stops forwarding with device-access-policy config
CSCvx68246	Changing Config-DB ID/Password from default to non-default on a cluster of more than 3 members

Compatibility Matrix and Server Recommendations

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

Related Documentation

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