Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.6.x

First Published: 2021-08-16

Last Modified: 2024-04-05

Read Me First



Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

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

User Documentation

- User Documentation for Cisco SD-WAN Release 20

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.

- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

Release Notes for Cisco vEdge Device, Cisco SD-WAN Release 20.6.x

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

These release notes accompany the Cisco SD-WAN Release 20.6.x, which provides Cisco Catalyst SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager as applicable to Cisco vEdge devices.

Related Releases

For release information about Cisco IOS XE Catalyst SD-WAN devices, refer to Release Notes for Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.6.x.

For release information about Cisco Catalyst SD-WAN Control Components, refer to Release Notes for Cisco Catalyst SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.6.x

What's New for Cisco SD-WAN Release 20.6.x

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 20.6.4

Feature	Description
Configure Disaster Recovery Alerts	This feature provides support for configuring Cisco SD-WAN Manager alerts to generate an alarm and a syslog message for any disaster recovery workflow failure or event that occurs.

Feature	Description
Renew Device CSR	This feature allows you to reset the RSA private and public keys, and generate a CSR that uses a new key pair. In earlier releases, the generation of CSR used the existing key pair.

Table 2: Cisco SD-WAN Release 20.6.2

Feature	Description
Support to Configure NTP Server using Localized Policy CLI	This feature allows you to configure the NTP server feature on Cisco SD-WAN devices using the Cisco SD-WAN Manager localized CLI policy.

Table 3: Cisco SD-WAN Release 20.6.1

Feature	Description
Cisco Catayst SD-WAN Getting Started	
Cisco SD-WAN Manager Persona-based Cluster Configuration	Simplifies adding Cisco SD-WAN Manager servers to a cluster by identifying servers based on personas. A persona defines what services run on a server.
Support for Reverse Proxy with Cisco IOS XE Catalyst SD-WAN Devices and Cisco SD-WAN Multitenancy	With this feature, you can deploy a reverse proxy device in your overlay network between Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Manager and Cisco SD-WAN Controller. Also, this feature enables you to deploy a reverse proxy device in both single-tenant and multitenant overlays that include Cisco vEdge or Cisco IOS XE Catalyst SD-WAN edge devices.
Systems and Interfaces	
Dual Endpoint support for interface status tracking on Cisco vEdge devices	This feature allows you to configure tracker groups with dual endpoints using the Cisco SD-WAN Manager System template and associate each template group to an interface. The dual endpoints provide redundancy for tracking the status of transport interfaces to avoid false negatives.
RBAC for Policies	This feature allows you to create users and user groups with required read and write permissions for Cisco SD-WAN Manager policies. RBAC for policies provides users with the access to all the details of policies to help maximize the operational efficiency. It makes it easier to meet configuration requirements and guarantees that authorized users on the system are only given access to what they need.
Tenant Device Forecasting	With this feature, a service provider can control the number of WAN edge devices a tenant can add to their overlay network. By doing so, the provider can utilize Cisco Catalyst SD-WAN control components resources efficiently.

Feature	Description
Migrate Multitenant Cisco Catalyst SD-WAN Overlay	This feature enables you to migrate a multitenant Cisco Catalyst SD-WAN overlay comprising shared Cisco SD-WAN Manager instances and Cisco SD-WAN Validator, and tenant-specific Cisco SD-WAN Validator to a multitenant overlay comprising shared Cisco SD-WAN Manager instances, Cisco SD-WAN Validator, and Cisco vSmart Controllers.
Routing	
Route Manipulation for Leaked Routes with OMP Administrative Distance	This feature allows you to configure the OMP administrative distance option to prefer OMP routes over MPLS routes.
Policies	
Traffic Classification Using NBAR	This feature extends Network-Based Application Recognition (NBAR) support to Cisco SD-WAN vEdge devices.
SLA Class Support Enhancement	This feature is an enhancement to support more than six SLA classes per policy on Cisco SD-WAN devices.
Application-aware Routing and Data Policy SLA Preferred Colors	This feature provides different behaviors to choose preferred colors based on the SLA requirements when both application-aware routing policy and data policies are configured.
Cisco Catalyst SD-WAN Security	
Authentication Types	The authentication types supported from Cisco SD-WAN Release 20.6.1 differ from the authentication types supported in Cisco SD-WAN Release 20.5.1 and earlier releases. For a Cisco vEdge device running Cisco SD-WAN Release 20.5.1 or earlier, if you have configured authentication types using the Cisco Security feature template, you must update the the authentication types in the template after you upgrade the device software to Cisco SD-WAN Release 20.6.1 or later. To update the authentication types, do the following: **1.** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**. **2.** Click **Feature Templates**. **3.** Find the **Security** template to update and click … and click **Edit**. **4.** Click **Update**. Do not modify any configuration. Cisco SD-WAN Manager updates the **Security** template to display the supported authentication types.
Cloud OnRamp	

Feature	Description
Cloud onRamp for SaaS over SIG Tunnels	This feature allows you to connect to Cloud onRamp for SaaS by means of a SIG tunnel. Cloud onRamp for SaaS over SIG tunnels provides you secure access to the SaaS applications, and the capability to automatically select the best possible SIG tunnel for accessing the SaaS applications.
Cisco Catalyst SD-WAN Monitor and Maintain	
Generate System Status Information for a Cisco SD-WAN Manager Cluster Using Admin Tech	This feature adds support for generating an admin-tech file for a Cisco SD-WAN Manager cluster. The admin-tech file is a collection of system status information intended for use by Cisco Catalyst SD-WAN Technical Support for troubleshooting. Prior to this feature, Cisco Catalyst SD-WAN was only able to generate an admin-tech file for a single device.
View Generated Admin-Tech Files at Any Time	This feature adds support for viewing generated admin-tech files whenever the admin-tech files are available on a device. You can view the list of generated admin-tech files and then decide which files to copy from your device to Cisco SD-WAN Manager. You can then download the selected admin-tech files to your local device, or delete the downloaded admin-tech files from Cisco SD-WAN Manager, the device, or both.
Embedded Packet Capture for Cisco vEdge Devices Using CLI Commands	This feature provides an alternative method to capture traffic data to troubleshoot connectivity issues between Cisco vEdge devices and Cisco SD-WAN Manager using supported CLI commands. As part of this feature, the following commands are introduced to capture traffic details: - request stream capture - show packet-capture details
Additional Real Time Monitoring Support for Routing, License, Policy, and Other Configuration Options	This feature adds support for real time monitoring of numerous device configuration details including routing, license, policy, Cloud Express, Cisco SD-WAN Validator, TCP optimization, SFP, tunnel connection, license, logging, and Cisco Umbrella information. Real time monitoring in Cisco SD-WAN Manager is similar to using **show** commands in the CLI of a device. There are many device configuration details for Cisco SD-WAN Manager. Only a subset of the device configuration details is added in Cisco IOS XE Release 17.6.1a and Cisco vManage Release 20.6.1.
Manage Data Collection for Cisco Catalyst SD-WAN Telemetry	This feature allows you to disable data collection for Cisco Catalyst SD-WAN telemetry using Cisco SD-WAN Manager. Data collection for telemetry is enabled by default.
On-Demand Troubleshooting	This feature lets you view detailed information about the flow of traffic from a device. You can use this information to assist with troubleshooting.
Production Change Management in Audit Logs	This feature adds support to include template and policy configuration details in audit logs. You can view the current and previous configuration details for any action in Cisco SD-WAN Manager.

Feature	Description
DPI Statistics	This feature lets you view detailed information about the flow of traffic from a device.
Cisco Catalyst SD-WAN SNMP	
Support for Cisco SD-WAN Traps	This feature adds support for receiving the following SNMP trap notifications: • Certificate expiration notification on Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices. • Health monitoring notifications on Cisco vEdge devices, Cisco SD-WAN Validator, Cisco SD-WAN Controller, and Cisco SD-WAN Manager.

Important Notes, Known Behavior, and Workaround

- Starting from Cisco SD-WAN Release 20.5.1, Cloud onRamp for IaaS isn't supported for Cisco vEdge Cloud Router running on Cisco SD-WAN Release 20.5.1. However, Cloud onRamp for IaaS is supported with AWS as the cloud provider for Cisco vEdge Cloud Routers using Cisco SD-WAN Release 20.4.1 and earlier. Cloud onRamp for IaaS is also supported with Microsoft Azure as the cloud provider for Cisco vEdge Routers using Cisco SD-WAN Release 20.3.1 and earlier.
- In Cisco SD-WAN Release 20.5.1, the cloud-init bootstrap configuration that you generate for the Cisco vEdge Cloud Router cannot be used for deploying the Cisco Cloud vEdge Router running on Cisco SD-WAN Release 20.5.1. However, you can use the bootstrap configuration for deploying the Cisco vEdge Cloud Router running on Cisco SD-WAN Release 20.4.1 and earlier versions.
- Cisco vManage Release 20.3.1 implements a hardened security posture to comply with FedRamp guidelines. As a result, your vAnalytics login credentials that are stored locally get erased on upgrading the software, and you cannot access the vAnalytics service directly through Cisco SD-WAN Manager. In this case, log in to vAnalytics using this URL: https://analytics.viptela.com. If you can't find your vAnalytics login credentials, open a case with Cisco TAC support.
- For Cisco SD-WAN Release 20.4.1, you must run the messaging server on all the active instances of the Cisco SD-WAN Manager cluster when deploying the Cisco SD-WAN Manager cluster. See the High Availability Configuration Guide for vEdge Routers for more information.
- For information about upgarde paths, see Cisco vManage Upgrade Paths.

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 20.6.7

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 20.6.7

Identifier	Headline
CSCwe21563	Cisco vEdge device cannot resolve Cisco SD-WAN Validator on the loopback interface.
CSCwf97711	On Cisco vEdge 1000 device, customer is seeing the clock getting reset after RTC reports PWRFAIL.
CSCwf80551	Cisco vEdge device symnat flag got stuck even when not behind nat.
CSCwf74787	Cisco vEdge device is crashing due to FP Core dying.
CSCwf54032	The "show bfd history" is not showing the "up" status after BFD tunnel recovers from flapping on Hub Cisco vEdge device.
CSCwf47529	BFD Tunnel convergence is taking couple more seconds longer.
CSCwe90126	Cisco ISR1100 : Interface went up/down state with speed 100m and no auto-neg configured post upgrade to 20.6
CSCwh63730	Cisco vEdge device version 20.6.5.3 are not generating Alarms for High CPU.

Bugs for Cisco SD-WAN Release 20.6.6

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 20.6.6

Identifier	Headline
CSCwf65485	Interface diagnostic commands won't show desired output on code 20.6.3.2 for Cisco vEdge-2000.
CSCwe86766	Current flows are not getting cleared post disabling app-visibility.
CSCwa78672	20.8: On-Demand tunnel not coming up between Cisco vEdge device and Cisco IOS XE Catalyst SD-WAN device sites.
CSCwe41667	Cisco vEdge-1000/ 20.6.5 / SSHd and vConfd spiking CPU up to 100%.
CSCwf70034	The DNS Cache populating without a valid response.
CSCwh24251	I2C bus gets hang leading h/w operation application failiure on 20.6
CSCwe80168	Cisco vEdge-2000 ftmd daemon crash. Signal 10.
CSCwe42133	Cisco vEdge device: Same label is assigned to different vpns.
CSCwf24092	Tracker on Cisco vEdge device does not come up after reboot.

Open Bugs for Cisco SD-WAN Release 20.6.6

Identifier	Headline
CSCwf97711	On Cisco vEdge-1000, Customer is seeing the clock getting reset after RTC reports PWRFAIL.
CSCwh36048	Port number that is lower than 1024 are chosen as the DIA NAPT source port in Cisco vEdge device.
CSCwh24273	Cisco vEdge-2000 - Fiber interfaces go down randomly.
CSCwf54032	The "show bfd history" not showing the "up" status after BFD tunnel recovers from flapping on Hub Cisco vEdge device.
CSCwf68248	Cisco vEdge-5000 upgrade failure from 20.6 to 20.9
CSCwf68816	High CPU in Cisco vEdge device caused by minigzip process.
CSCwa23852	Microsoft Azure: Cisco vEdge device/Cisco Catalyst SD-WAN Controller VHD image doesn't prompt initial admin password wizard.
CSCwh57463	[SITLite] After deconfigure ipsec+pwk , unable to recover all bfd sessions

Bugs for Cisco SD-WAN Release 20.6.5.4

Resolved Bugs for Cisco SD-WAN Release 20.6.5.4

Identifier	Headline
CSCwf34096	Cisco vEdge 5000 device inbuilt certificate expiring on 12th November 2023

Bugs for Cisco SD-WAN Release 20.6.5.3

Resolved Bugs for Cisco SD-WAN Release 20.6.5.3

Identifier	Headline
CSCwd85558	The app-server java process is not initiating in 6 node 20.6 cluster
CSCwe12396	The max netconf sessions reached in confd which causes login failure for vManage
CSCwd57223	Cisco vEdge upgrade from 20.3.4 to 20.6.3 failed
CSCwd17126	Cisco vEdge: TLS control connections flapping with vSmart upgraded to 20.6
CSCwe26011	Cisco SD-WAN Manager is not generating alarm notifications to be sent to Webhooks server.
CSCwd85846	The DTLS session with the vBond does not come up due to OOO packets received at the vEdge
CSCwd54202	The IGMP not receiving joins after upgrading to 20.6.4

Identifier	Headline
CSCwf28118	Cisco vEdge: Certificate issue on Cisco vEdge devices

Bugs for Cisco SD-WAN Release 20.6.3.3

Resolved Bugs for Cisco SD-WAN Release 20.6.3.3

Identifier	Headline
CSCwd18230	The duplicate entries of interface seen multiple VPN on performing reboot/upgrade
CSCvz44093	[SIT] core.vtracker file found on Cisco vEdge 1000
CSCwc63734	The 20.9 -Edit template lock and FSM stuck state issue
CSCwb39498	The time out : no response seen on running SNMPwalk on Cisco vEdge 5000
CSCwa84441	The IKEv2/vEdge long failover time
CSCwd46600	Cisco vEdge: Data traffic loss was seen because of IPsec RX Auth Failures and Window drops
CSCwc31458	The shaping-rate is programmed to another interface in the same VPN.
CSCwd57223	Cisco vEdge upgrade from 20.3.4 to 20.6.3 failed
CSCwc80831	The high CPU seen across vEdge platform
CSCwf28118	Cisco vEdge: Certificate issue on Cisco vEdge devices
CSCwb03242	The Cisco vEdge routing table did not remove deleted default route
CSCwc78553	On doing OIR for 1G Fiber SFP, interface is not coming up
CSCwd33072	Cisco vEdge 5000 "fp_dump -ec" CLI Corrupts Forwarding Cores
CSCwb04644	The SNMPD crash seen on running Snmpwalk - 20.6.2 Cisco vEdge 5000
CSCwc31839	Cisco vEdge 5000 interface not coming up post shut/un-shut
CSCwc78699	The ZIA not re-trying request to zscalar if the WAN interface gets an ip address with a little delay.
CSCwb21516	Cisco vEdge 1000: Multiple crash seen on Cisco vEdge 1000 with DPI enabled and Scaled flows

Bugs for Cisco SD-WAN Release 20.6.1.2

Resolved Bugs for Cisco SD-WAN Release 20.6.1.2

Identifier	Headline
CSCwf28118	Cisco vEdge: Certificate issue on Cisco vEdge devices

Bugs for Cisco SD-WAN Release 20.6.4.1

Resolved Bugs for Cisco SD-WAN Release 20.6.4.1

Identifier	Headline
CSCwf28118	Cisco vEdge: Certificate issue on Cisco vEdge devices

Bugs for Cisco SD-WAN Release 20.6.5.2

Resolved Bugs for Cisco SD-WAN Release 20.6.5.2

Identifier	Headline
CSCwf28118	Cisco vEdge: Certificate issue on Cisco vEdge devices

Bugs for Cisco SD-WAN Release 20.6.3.2

Resolved Bugs for Cisco SD-WAN Release 20.6.3.2

Identifier	Headline
CSCwf28118	Cisco vEdge: Certificate issue on Cisco vEdge devices

Bugs for Cisco SD-WAN Release 20.6.5

Resolved Bugs for Cisco SD-WAN Release 20.6.5

Identifier	Headline
CSCwd18230	Duplicate entries of interface seen multiple VPN on performing reboot/upgrade
CSCwc62342	Cisco vEdge devices pimd crash on 20.3.5
CSCwd33072	Cisco vEdge devices 5K "fp_dump -ec" CLI Corrupts Forwarding Cores
CSCwc31458	Shaping-rate is programmed to another interface in the same VPN.
CSCwc80831	High CPU seen across Cisco vEdge devices platform
CSCwc78553	On doing OIR for 1G Fiber SFP, interface is not coming up
CSCwc63734	20.9 -Edit template lock and FSM stuck state issue
CSCwd43784	APP Engine ID wrongly set to 0 - invalid (0)
CSCwd46600	Cisco vEdge devices: Data traffic loss was seen because of IPsec RX Auth Failures and Window drops
CSCwc31839	Cisco vEdge devices 5k interface not coming up post shut/un-shut

Identifier	Headline
CSCwc78699	ZIA not re-trying request to zscalar if the WAN interface gets an ip address with a little delay.
CSCwd46921	Cisco vEdge devices is not connecting to second vSmart after both assigned Cisco SD-WAN Controller is down
CSCwc57970	"Error in packet.: (genError) A general failure occured" seen when running snmpwalk on Cisco vEdge devices-cloud

Open Bugs for Cisco SD-WAN Release 20.6.5

Identifier	Headline
CSCwd70324	LSC Interrupts not seen for interface post reboot and interfave protocol status remians down
CSCwd57223	Cisco vEdge devices upgrade from 20.3.4 to 20.6.3 failed
CSCwd86981	Wrong reboot reason reported when Cisco vEdge devices 2k/1k goes for unexpected reboot
CSCwd17126	Control Connections flapping after Cisco SD-WAN Controller upgrade to 20.6.2 version when using tls.
CSCwd85853	Cisco vEdge devices 2000 reloads without generating a core file
CSCwa23852	Azure Viptela Cisco vEdge devices/vSmart VHD image doesn't prompt initial admin password wizard

Bugs for Cisco SD-WAN Release 20.6.4

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 20.6.4

Identifier	Headline
CSCvz64630	Enhancement request to restrict access to GDB tool for non root users. i.e. restrict to 0700
CSCvz44093	[SIT] core.vtracker file found on Cisco vEdge devices 1000
CSCwb48785	Getting "Error in packet.: (genError) A general failure occured" when running snmpwalk on Cisco vEdge devices
CSCwa84441	IKEv2/Cisco vEdge devices long failover time
CSCwb06217	After failover Existing primary Cisco vEdge devices stops receiving traffic and forwarding - 20.6.2

Identifier	Headline
CSCwa82541	Cisco vEdge devices: ECMP for DP based DIA is not maintained if AAR policy applied
CSCwa51818	Cisco vEdge devices-5000 not able to configure more than 4 SLA's
CSCwb04644	SNMPD crash seen on running Snmpwalk - 20.6.2 Cisco vEdge devices5K
CSCwa92331	Affinity logic not working if entire CG1 vsmarts shutdown
CSCwa67563	Cisco vEdge devices USB directory requires root access on 20.6
CSCwc07584	Supress Sysmgr sig 9 from hitting wtmp history post killing critical process
CSCwa92675	Cisco vEdge devices-100 will not boot after a power cycle if connected to a terminal server
CSCwb39731	Cisco vEdge devices 5K: Fragmented packets don't get transmitted out of the device

Open Bugs for Cisco SD-WAN Release 20.6.4

Identifier	Headline
CSCwa36262	Cisco vEdge devices 1000 after upgrading to 20.6.1 Error: application communication failure is seen
CSCwc64459	20.3.x Cisco vEdge devices SNMP template push failing from 20.6 Cisco SD-WAN Manager after 1st successful push
CSCwc53455	Cisco vEdge devices dns-redirect is not workling with Zscaler
CSCwc04078	Cisco vEdge devices 1K silent reboot Warm Reset(CHIP RESET)
CSCwc31839	Cisco vEdge devices5k interface not coming up post shut/un-shut
CSCwc42336	Cisco vEdge devices cloud will rename ge interface as eth interfaces on 20.6.3 on openstack hypervisor
CSCwa23852	Azure Viptela Cisco vEdge devices/vSmart VHD image doesn't prompt initial admin password wizard
CSCwd85121	After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.

Bugs for Cisco SD-WAN Release 20.6.3

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 20.6.3

Bug ID	Description
CSCwa58714	Loopback interface not reachable when the gateway set to the virtual vrrp ip

CSCwa08989	Interested traffic(FTP/SIP/ICMP...) can't be forwarded properly after Cisco vEdge Device devi
CSCwa32952	Cisco vEdge Device access controlled via TACACS+ prevents user from performing certain co
CSCwa78885	Cisco vEdge Device 2k crashed due to kernel panic while generated admin-tech from Cisco SI
CSCvz42160	Device not rebooting after an intentional crash
CSCvy27321	Cisco vEdge Device interface tracker reporting down status in vdebug constantly while on the
CSCvz87934	Cisco vEdge Device marking the routes as invalid in OMP when the control policy is changed.
CSCwa84507	Hardware Random Number generation shouldn't include TPM RNG until mutexing occurrs
CSCvy57380	Endpoint Tracker stays down when ip address changed from dhcp to static
CSCwa59201	Cisco vEdge Device 5k TPM failure resulting TLOC disable
CSCwa24992	ZBFW zone-pair (service to service) not working as expected.
CSCwa01810	Affinity on Cisco vEdge Device will fulfill EQUILIBRIUM when it loses the included vSmart

Open Bugs for Cisco SD-WAN Release 20.6.3

Bug ID	Description
CSCwb55433	Cisco vEdge Devicenot accepting 2 static routes if one of them is Null0
CSCwa92331	Affinity logic not working if entire CG1 vsmarts shutdown
CSCwb06217	After failover Existing primary Cisco vEdge Device stops receiving traffic and forwarding - 20
CSCwb57899	Cisco vEdge Device: fails to reboot automatically after FP watchdog failure
CSCwa23852	Azure Cisco SD-WAN Cisco vEdge Device/Cisco Catalyst SD-WAN Controller VHD image d
CSCwd85121	After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.

Bugs for Cisco SD-WAN Release 20.6.2

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 20.6.2

Bug ID	Description
CSCvy37285	SSH to Loopback not working
CSCvy89362	QOS-3-INVALID_BQS_QUEUE_INFO: Drop policy given an invalid scheduling queue/wred 0/0 -Traceback
CSCvy91411	Cisco Catalyst SD-WAN policy is not correctly programmed in Cisco IOS XE Catalyst SD-WAN device

Bug ID	Description
CSCvy92960	C8500 QFP FirewallNonsession drops when starting 80K flows
CSCvy97761	IPV6 route is breaking control connection.
CSCvy98784	AppQoE DP stats for active connections shows huge bogus value
CSCvy99344	Cisco IOS XE Catalyst SD-WAN device: Multicast UnconfiguredIpv4Fia drop when multicast interworks with service chain/NAT DIA
CSCvz03053	OMP continues to redistribute BGP route with down bit set (SoO)
CSCvz04121	"show sdwan tunnel statistics bfd" and "clear sdwan tunnel statistics" issues
CSCvz09330	Bootstrap aaa config issues due to default aaa config
CSCvz23024	17.6.1_auto:SNMP failure on bfdSessionsListSystemIp
CSCvz25619	FNF: Reload due to a memory allocation failure in Cisco IOS XE Catalyst SD-WAN device
CSCvz30465	MT: Template push with thousand eye feature failed for ISR4461 after PnP workflow
CSCvz38312	ISR1100 - Cisco IOS XE Catalyst SD-WAN device: Tx queue hang issue on RJ45 ports
CSCvz40788	Cisco Catalyst SDWAN tunnels are not coming up in Multilink Frame relay sub-interface
CSCvz45159	Data plane crash seen on C8200-UCPE-1N8 with upgrade of c8kv from 17.5.1 to 17.6.1 build
CSCvz47982	Flow-Control Goes down when configurating manual speed and remove the auto negotiation
CSCvz55789	Data-policy direction-all with empty action is causing to ignore app-route-policy
CSCvz56966	Zscaler SIG tunnels not coming up after reboot due to HTTP/RESP/CODE 400
CSCvz62602	Extranet local switch crash when mdata is enabled.
CSCvz69124	ISR4k:BFD scaling: Not able to scale more that 2048 BFD sessions
CSCvz70734	Cisco IOS XE Catalyst SD-WAN device crash with sdwan overlay multicast: "CPU Usage due to Memory Pressure exceeds threshold"
CSCvz70426	VEdge VRRP-VIP IP address not responding in multi VPN
CSCvz86967	vEdge DST Root CA X3 Expiration causing umbrella integration to fail
CSCvz65048	vEdge 20.6.1: Locally sourced DNS packets uses incorrect interface while resolving Cisco Catalyst SD-WAN Validator hostname.
CSCvz83560	vEdge 20.6.1: Control connection fails to come up due to DTLS handshake failure.

Bug ID	Description
CSCvz65300	vEdge 20.6.1: BGP route is not considered to reach DNS server during Cisco Catalyst SD-WAN Validator hostname DNS lookup
CSCvy46919	vEdge: Out of Order IKE Negotiation causes IKE to get stuck

Open Bugs for Cisco SD-WAN Release 20.6.2

Bug ID	Description
CSCvz42885	Packet drops due to QoS Policy after upgrading from 20.3.3 to 20.6.0.101
CSCwa25457	Nutella 6G/Vedge 5K: BFD sessions take long time to come up after clearing omp sessions
CSCvz46516	sit_regression; speedtest.py- test_speedtest_2edges: Failed to start iperf client
CSCwa23852	Azure Viptela vEdge/vSmart VHD image doesn't prompt initial admin password wizard
CSCwd85121	After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.

Bugs for Cisco SD-WAN Release 20.6.1

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 20.6.1

Bug ID	Description
CSCvw31987	Cisco vEdge 1000 rebooted with Software initiated - Daemon 'ftmd' failed
CSCvw54152	Cisco vEdge 5k-LLQ policer rate on interface 10ge0/0 change after reboot on version 20.1.932
CSCvx18309	Cloud-init tries to configure dhcp ip on eth0 interface on ESXI (support VMware*)
CSCvx26199	Control connection to Cisco vManage does not failover from IPv6 interface to IPv4 interface
CSCvx44834	ASR1K - ACE entry added after object-group is missing in hardware causing packets drops
CSCvx50343	Routes redistributed to the OSPF/BGP that shouldn't be filtered by the routing-policy are filtered
CSCvx83356	Global Route leaking feature do not import routes if the route policy name is lengthy
CSCvx84040	Cisco vEdge running 19.2.31 crashes with dbgd failed message while doing speed test
CSCvx85654	shaping-rate value on main interface doesn't apply on traffic through sub interface on Cisco vEdge 5k

Bug ID	Description
CSCvx86673	Cisco vEdge show interface command shows wrong information for speed
CSCvy02586	Additional counter to capture the mismatch between control and data plane hash table ZBF records.
CSCvy03463	FTMD crash seen after customer tried to add a second tracker to an interface
CSCvy08650	In 20.3.2.1 transport interface distribution, view percentage utilization shows blank
CSCvy14007	Cisco vEdge:PIMD crash after few min of multicast traffic received
CSCvy18908	Cloud Cisco vEdge crash on bfdmgr_update_sla_mapping
CSCvy33818	On MTT Cisco vManage system IP persists after invalidating and deleting the edge devices.
CSCvy65611	Cisco vEdge-2000 dropping arp replies post upgrading to 20.5.1
CSCvy83632	DNS resolution fails from VPN 511 - request download vpn 511 <URL>
CSCvy86565	[20.6.1-EFT] vBond Software upgrade from SW ver 20.3 to 20.6.1 EFT image is failing
CSCvz30626	20.6: Cisco vManage Main Dashboard , with Top Application Data => SSL proxy, data is empty

Open Bugs for Cisco SD-WAN Release 20.6.1

Bug ID	Description
CSCvx44834	ASR1K - ACE entry added after object-group is missing in hardware causing packets drops
CSCvy33818	On MTT Cisco vManage system IP persists after invalidating and deleting the edge devices.
CSCvy66289	Cisco vEdge not initiating arp request after upgrading
CSCvz00831	Nutella 6G/Cisco vEdge 5K: BFD sessions take hours to come up after clearing omp sessions
CSCvz01685	Set local tloc does not respect DPI sticky rule
CSCvz21798	Cisco vEdge CLoud Heat template is chaning Interface names on SW Version 20.5
CSCvz30626	20.6: Cisco vManage Main Dashboard , with Top Application Data => SSL proxy, data is empty
CSCwd85121	After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.

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.

Supported Devices

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

Redesign of Cisco SD-WAN Manager GUI

From Cisco vManage Release 20.6.1, Cisco SD-WAN Manager GUI is redesigned and offers a new visual display. Besides the new sign in screen, this section presents a comparative summary of the significant changes between older Cisco vManage releases and Cisco vManage Release 20.6.1 and later.

Change in Navigation Menu

From Cisco vManage Release 20.6.1, the navigation menu at the top left of the Cisco SD-WAN Manager window is collapsed, and can be expanded to view the menu options. The previous releases of Cisco SD-WAN Manager have a static side-bar navigation menu.

Figure 1: Navigation Menu in Cisco vManage Release 20.5.1 and Earlier

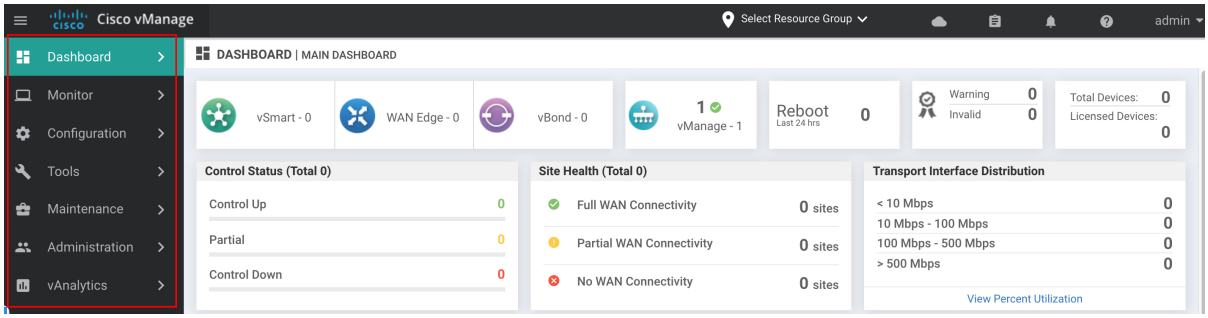


Figure 2: Navigation Menu (Collapsed) in Cisco vManage Release 20.6.1 and Later

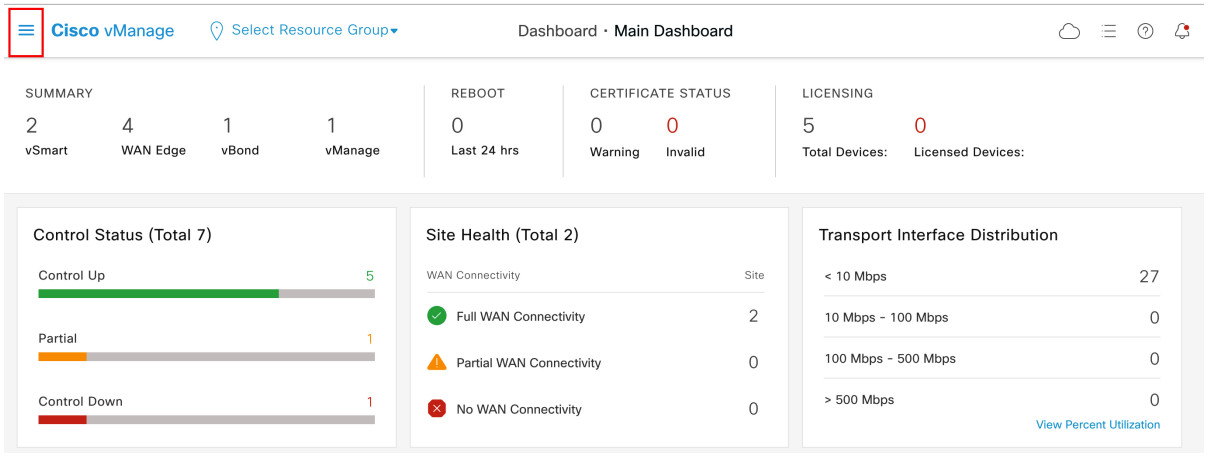
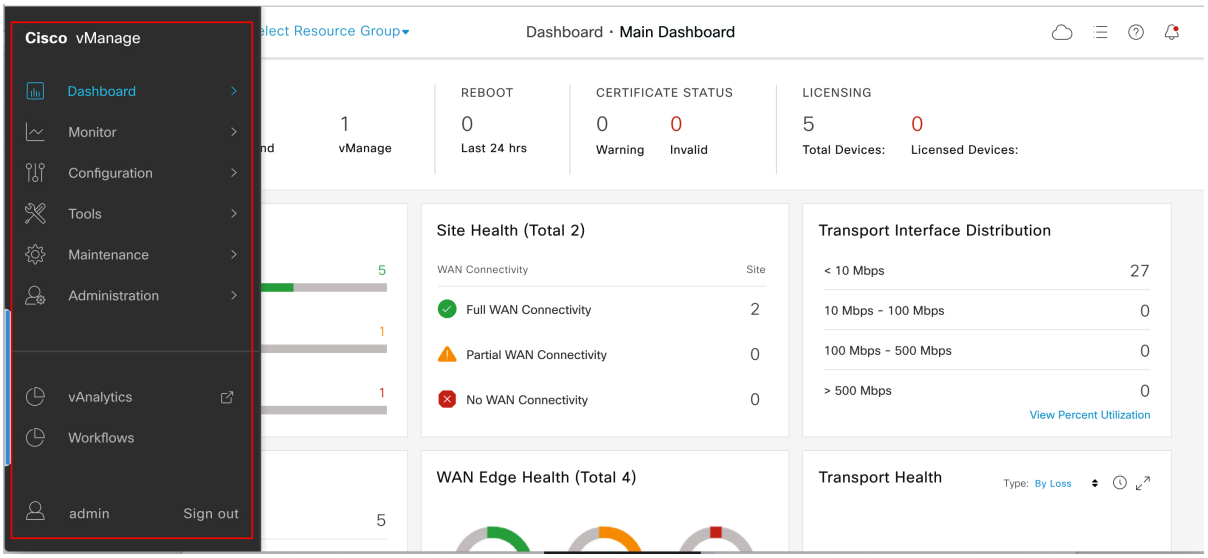


Figure 3: Navigation Menu (Expanded) in Cisco vManage Release 20.6.1 and Later



Change in Position of the User Profile and Sign Out Options

From Cisco vManage Release 20.6.1, the **User Profile** and **Sign Out** options are moved to the bottom of the collapsible side-bar menu in the left pane. In the previous releases, these options are available at the top-right corner of Cisco SD-WAN Manager.

Figure 4: User Profile and Sign Out Options inCisco vManage Release 20.5.1 and Earlier

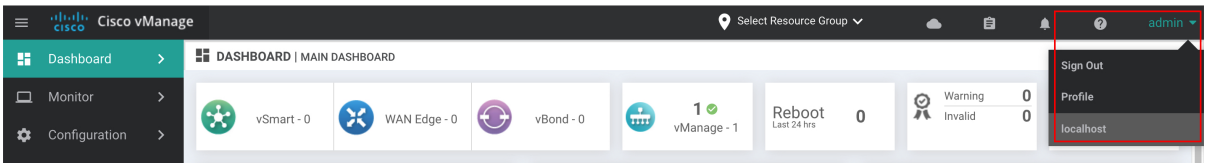
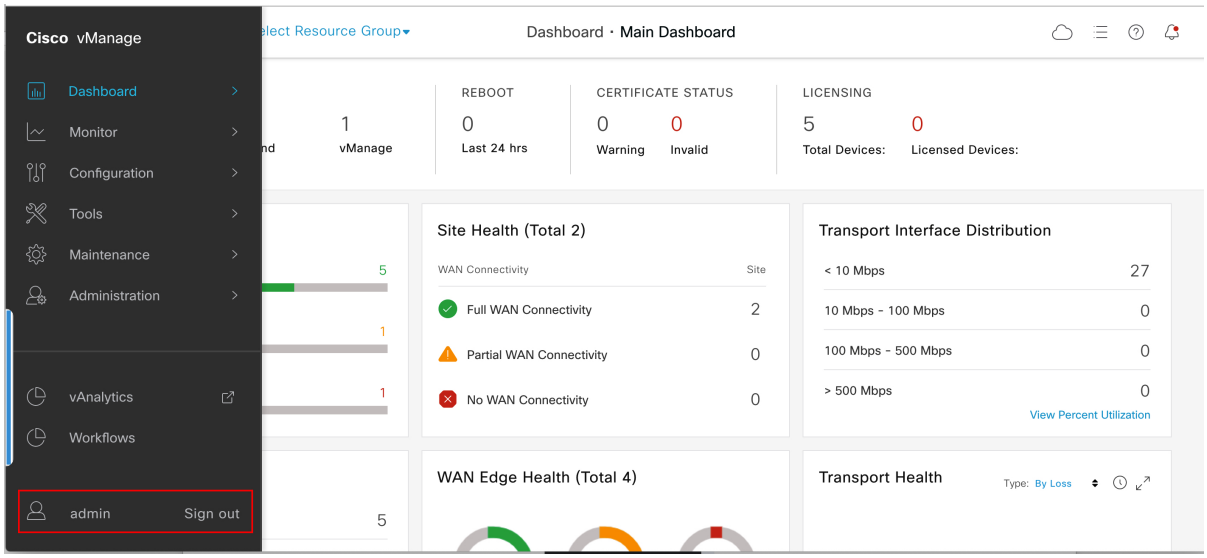


Figure 5: User Profile and Sign Out Options in Cisco vManage Release 20.6.1 and Later



Change in Presentation of the Main Dashboard

From Cisco vManage Release 20.6.1, the position of **Select Resource Group** drop-down menu is shifted to the left.

Figure 6: Main Dashboard in Cisco vManage Release 20.5.1 and Earlier

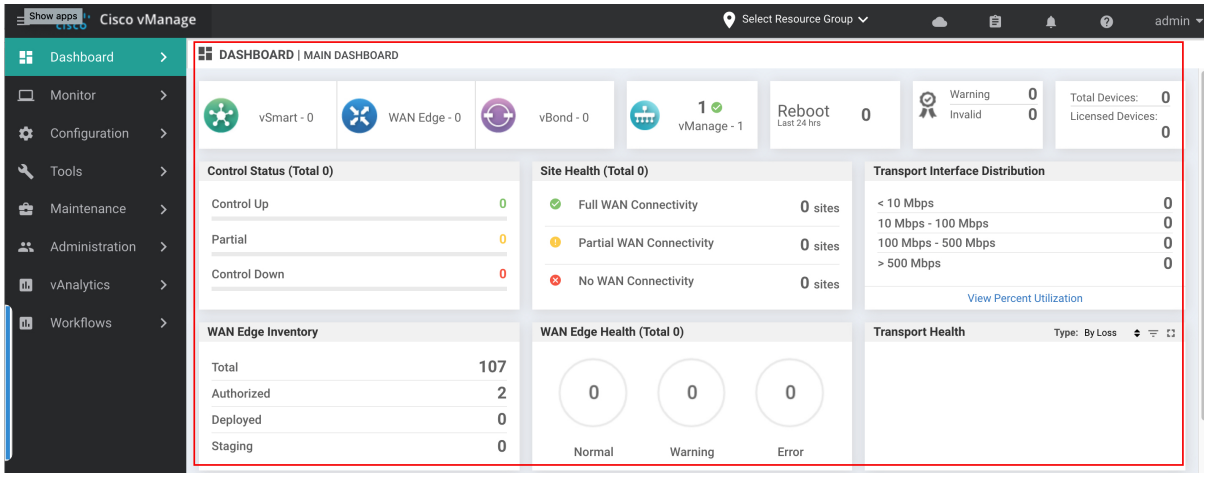
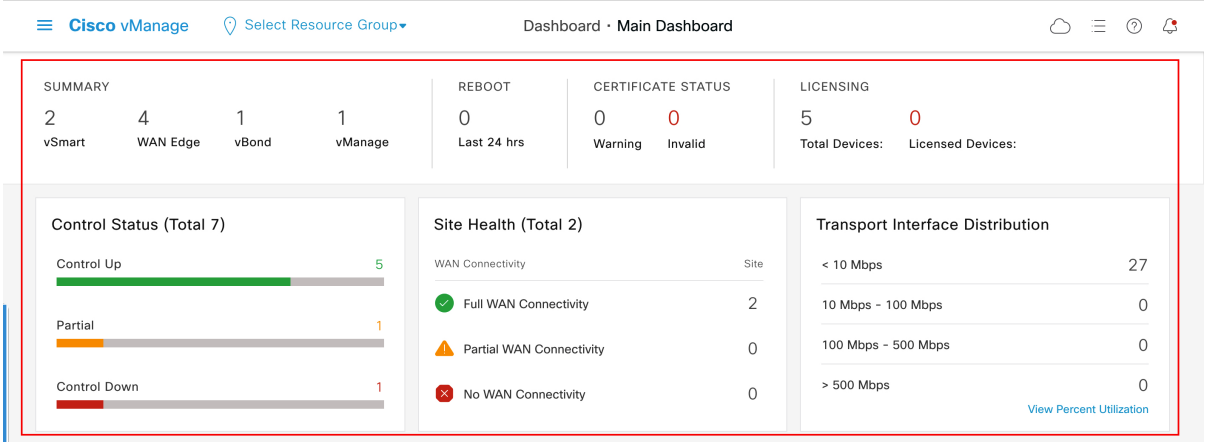


Figure 7: Main Dashboard in Cisco vManage Release 20.6.1 and Later



Other Changes

The redesign includes:

- New icons across Cisco SD-WAN Manager

Figure 8: Example of Icons in Cisco vManage Release 20.5.1 and Earlier

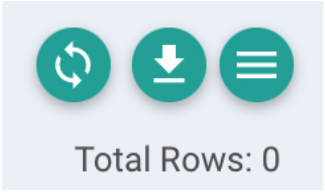


Figure 9: Example of Icons in Cisco vManage Release 20.6.1 and Later



- New design for GUI elements such as tabs and buttons

Figure 10: Example of GUI Elements in Cisco vManage Release 20.5.1 and Earlier

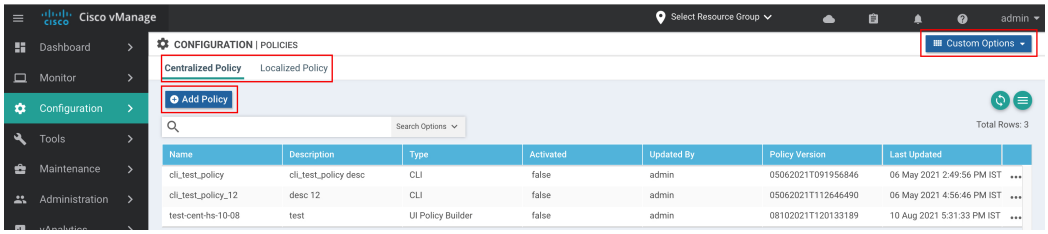
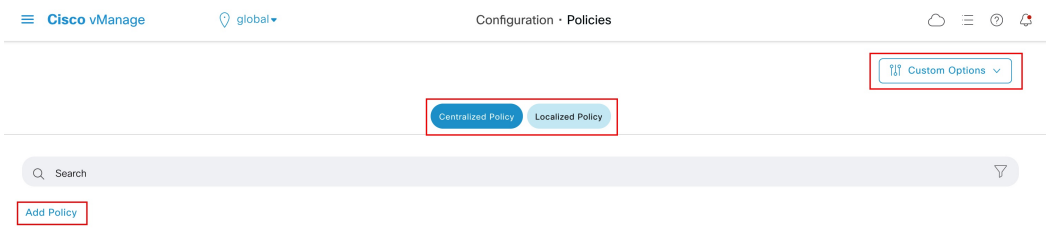


Figure 11: Example of GUI Elements in Cisco vManage Release 20.6.1 and Later



- New design for search bars across Cisco SD-WAN Manager

Figure 12: Example of Search Bar in Cisco vManage Release 20.5.1 and Earlier

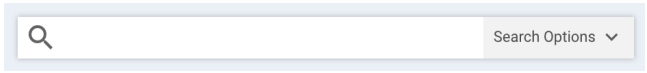
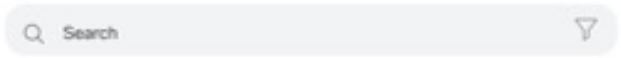


Figure 13: Example of Search Bar in Cisco vManage Release 20.6.1 and Later



Related Documentation

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

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.