Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.6.x

First Published: 2021-08-16

Last Modified: 2024-10-16

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 IOS XE Catalyst SD-WAN Release 17

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 IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.6.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 IOS XE Catalyst SD-WAN Release 17.6.x, which provides Cisco 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 IOS XE Catalyst SD-WAN devices.

Related Releases

For release information about Cisco vEdge Devices, refer to Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.6.x.

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

What's New for Cisco IOS XE Catalyst SD-WAN Release 17.6.x

This section applies to Cisco IOS XE Catalyst SD-WAN devices.

Cisco is constantly enhancing the Cisco Catalyst 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 IOS XE Catalyst SD-WAN Release 17.6.4

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.
Support for NAT High-Speed Logging	This feature provides the ability to enable or disable high-speed logging (HSL) of all translations by NAT. The new **ip nat log translations flow-export** command is introduced. You can configure NAT HSL using a device CLI or a CLI add-on template.
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.
DigiCert Migration	This feature enables Digicert certificate authority server in place of Symantec certificate authority server for signing the controller device certificates on Cisco SD-WAN Control Components including Cisco SD-WAN Controller, Cisco SD-WAN Validator, and Cisco SD-WAN Manager. You can protect, verify, and authenticate the identities of organizations and domains using these certificates.

Table 2: Cisco IOS XE Catalyst SD-WAN Release 17.6.2

Feature	Description
Layer 7 Health Check Support for SIG Tunnels for Umbrella and zScalar	This feature provides Layer 7 health check support for the SIG auto tunnels for Umbrella and Zscaler, in Cisco IOS XE Catalyst SD-WAN devices.

Table 3: Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started	
Quick Connect Workflow for Onboarding Cisco IOS XE Catalyst SD-WAN Devices	This feature provides an alternative, guided method in Cisco SD-WAN Manager to onboard supported WAN edge devices into the Cisco Catalyst SD-WAN overlay network. As part of the Quick Connect workflow, basic day-0 configuration profiles are created, which apply to all Cisco IOS XE Catalyst SD-WAN devices, irrespective of the device model and device family. This workflow adds edge devices to the WAN transport and establishes data plane and control plane connections. This feature is supported on Cisco IOS XE Catalyst SD-WAN devices only.
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.

Feature	Description
Support for Reverse Proxy with Cisco IOS XE Catalyst SD-WAN Devices and Cisco Catalyst 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.
Support for License Management Offline Mode and Compliance Alarms	With this feature, you can manage Cisco Catalyst SD-WAN licenses through a Cisco SD-WAN Manager instance that is not connected to the internet. To synchronize license and compliance information between Cisco SD-WAN Manager and Cisco SSM, you must periodically download synchronization files from Cisco SD-WAN Manager and upload the files to Cisco SSM. This feature also introduces compliance alarms that alert you if devices in the Cisco Catalyst SD-WAN network are not yet licensed.
Cisco Catalyst SD-WAN Systems and Interfaces	
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.
Implicit ACL on Loopback Interfaces	This feature allows you to configure implicit ACL on loopback interfaces. You can filter and manage data traffic by configuring implicit ACL on loopback interfaces instead of using the physical WAN interface. This saves public IP address space.
Geofencing	This feature provides a way to restrict a device's location to an operational geographical boundary, and to identify a device's location and report any violations of the configured boundary. If the device is identified to be in violation, you can restrict network access to the device using Cisco SD-WAN Manager operational commands. In the CLI or a CLI template, configure geofencing coordinates for establishing the location of the device. You can also register for SMS alerts.
Cisco Catalyst SD-WAN EtherChannel	This feature allows you to configure EtherChannels on Cisco IOS XE Catalyst SD-WAN devices in service-side VPN. An EtherChannel provides fault-tolerant high speed link, redundancy, and increased bandwidth between Cisco IOS XE Catalyst SD-WAN devices and other devices such as routers, switches, or servers connected in a network. You can configure EtherChannels only using the CLI device templates and CLI add-on feature templates.
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 Controller to a multitenant overlay comprising shared Cisco SD-WAN Manager instances, Cisco SD-WAN Validators, and Cisco SD-WAN Controllers.
Cisco Catalyst SD-WAN Support for Carrier Supporting Carrier Connectivity	The feature adds support for carrier supporting carrier (CSC) connectivity on Cisco IOS XE Catalyst SD-WAN devices. CSC enables you to interconnect IP or multiprotocol label switching (MPLS) networks operating at different sites over an MPLS backbone network. Using CSC requires an edge router that supports CSC functionality, called a carrier edge (CE) device, at each site. This feature enables a Cisco IOS XE Catalyst SD-WAN device to serve as a CE device, making it unnecessary to have a separate dedicated CE device at each site managed by Cisco Catalyst SD-WAN.
Wireless Management on Cisco 1000 Series Integrated Services Routers	This feature enables you to configure wireless LAN settings on Cisco 1000 Series Integrated Services using Cisco SD-WAN Manager. With Cisco SD-WAN Manager, you can automate the wireless LAN controller configuration and provide wireless connectivity without the need of another external controller to configure and manage wireless settings on the routers.
Extended Visibility with Cisco Catalyst SD-WAN and Cisco ThousandEyes	You can deploy Cisco ThousandEyes Enterprise agent natively as a container application on eligible Cisco IOS XE Catalyst SD-WAN devices to integrate Cisco SD-WAN Manager with Cisco ThousandEyes. You can install and activate the Cisco ThousandEyes Enterprise agent through Cisco SD-WAN Manager. By integrating Cisco Catalyst SD-WAN with Cisco ThousandEyes, you can gain granular insights into network and application performance with full hop-by-hop path analysis across the Internet, and isolate fault domains for expedited troubleshooting and resolution.
Cisco Catalyst SD-WAN Routing	
Radio-Aware Routing Support	This feature enables Radio-Aware Routing (RAR) support on Cisco IOS XE Catalyst SD-WAN devices. RAR is a mechanism that uses radios to interact with the routing protocol OSPFv3 to signal the appearance, disappearance, and link conditions of one-hop routing neighbors. In a large mobile networks, connections to the routing neighbors are interrupted due to distance and radio obstructions. RAR addresses the challenges faced when merging IP routing and radio communications in mobile networks.
Redistribution of Replicated Routes to BGP, OSPF, and EIGRP Protocols	This feature allows you to configure the following: - Redistribution of leaked or replicated routes between the global VRF and service VPNs for BGP, OSPF, and EIGRP protocols on Cisco IOS XE Catalyst SD-WAN device - OMP administrative distance option to prefer OMP routes over MPLS routes - VRRP tracking to track whether a leaked route is reachable
Cisco Catalyst SD-WAN Policies	

Feature	Description
SLA Class Support Enhancement	This feature is an enhancement to support more than six SLA classes per policy on Cisco IOS XE Catalyst SD-WAN device 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.
Flexible NetFlow Enhancement	This feature enhances Flexible NetFlow to collect type of service (ToS), sampler ID and remarked DSCP values in netflow records. This enhancement provides the flexibility to define flow record fields to customize flow records by defining flow record fields. The ToS and remarked DSCP fields are supported only on IPv4 records. However, the sampler ID field is supported for both IPv4 and IPv6 records.
Cisco Catalyst SD-WAN Security	
Unified Security Policy	This feature allows you to configure a single unified security policy for firewall and UTD security features such as IPS, Cisco URL Filtering, AMP, and TLS/SSL. Having a single unified security policy simplifies policy configuration and enforcement as firewall and UTD policies can be configured together in a single security operation rather than as individual policies.
Authentication Types	The authentication types supported from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a differ from the authentication types supported in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a and earlier releases. For a Cisco IOS XE Catalyst SD-WAN device running Cisco IOS XE Catalyst SD-WAN Release 17.5.1a 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 IOS XE Catalyst SD-WAN Release 17.6.1a 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 **Cisco Security** template to update and click … and click **Edit**. **4.** Click **Update**. Do not modify any configuration. Cisco SD-WAN Manager updates the **Cisco Security** template to display the supported authentication types.
Cisco Catalyst SD-WAN Cloud OnRamp	

Feature	Description
Support for Cloud OnRamp for SaaS Probing through VPN 0 Interfaces at Gateway Sites	Cloud OnRamp for SaaS tests the performance of (probes) routing paths to find the best routing path for specific cloud application traffic. Using the best routing path for the traffic of a cloud application optimizes the performance of the application. This feature enables Cloud OnRamp for SaaS to probe through VPN 0 interfaces at gateway sites as part of determining the best path to use for the traffic of specified cloud applications. This extends the best path probing to include more of the available interfaces connected to the internet. Using this feature, Cloud OnRamp for SaaS can probe interfaces at a gateway site, whether they use service VPNs (VPN 1, VPN 2, and so on) or the transport VPN (VPN 0). This is helpful when a branch site connects to the internet, exclusively or in part, through a gateway site that uses a VPN 0 interface to connect to the internet.
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.
Routing Traffic Flow to a Virtual Hub Firewall or a Local Firewall	This feature enables you to route Microsoft Azure Virtual WAN hub traffic to a firewall on a local branch router, or direct local branch traffic to an Azure secured virtual hub, to be subject to the security policies of the Azure Firewall Manager.
Cisco Catalyst SD-WAN and Google Service Directory Integration and Support for Cloud State Audit and Cloud Resource Inventory	With the integration of Google Service Directory with the Cisco Catalyst SD-WAN solution, you can discover your applications in the Google cloud using Cisco SD-WAN Manager. You can use the discovered applications to define application-aware routing policies in Cisco SD-WAN Manager. The Audit feature in Cisco SD-WAN Manager is now extended to Google Cloud integration. Use this option to ensure that the states of the objects in Google Cloud stay in sync with Cisco SD-WAN Manager state. Cloud Resource Inventory in Cisco SD-WAN Manager retrieves a detailed list of your cloud objects, their identifiers, the timestamps when such objects were created, and so on.
Cisco SD-WAN Manager Support for Monitoring Multicloud Services	This feature enables you to monitor your multicloud network using the Cisco SD-WAN Manager UI.
Cisco Catalyst SD-WAN Cloud Interconnect with Megaport: Interconnects to Google Cloud and Microsoft Azure	You can deploy a Cisco Catalyst 8000v Edge Software (Cisco Catalyst 8000V) instance as the interconnect gateway in the Megaport fabric and connect an Cisco Catalyst SD-WAN branch location to the interconnect gateway. From the interconnect gateway, you can create software-defined interconnects to Google Cloud VPCs, or Microsoft Azure VNets or Virtual WANs to link your branch location to the cloud resources through the Megaport fabric.

Feature	Description
Cisco Catalyst SD-WAN Cloud Interconnect with Equinix	You can deploy a Cisco Cloud Services Router 1000V (Cisco CSR 1000V) instance as the Interconnect Gateway in the Equinix fabric and connect an SD-WAN branch location to the Interconnect Gateway. From the Interconnect Gateway, you can create software-defined interconnects to an AWS cloud onramp or another interconnect gateway in the Equinix fabric.
Cisco Catalyst SD-WAN AppQoE	
DRE Profiles	This feature provides the flexibility to use resources for DRE based on your connection requirements by applying profiles such as S, M, L, and XL. Apply DRE profiles using the AppQoE feature template in Cisco SD-WAN Manager.
UCS-E Series Server Support for Deploying Cisco Catalyst 8000V	This feature lets you deploy Cisco Catalyst 8000V instances, on supported routers, using the UCS-E series blade server modules. With this feature, the supported routers can be configured as integrated service nodes, external service nodes, or hybrid clusters with both internal and external service nodes.
Enhanced Troubleshooting for AppQoE	This release introduces additional show commands to verify and troubleshoot issues in AppQoE features. A few existing show commands for AppQoE have also been enhanced. - show sdwan appqoe error recent - show sdwan appqoe status - show sdwan appqoe flow closed (command modified to include the keyword error) - show sslproxy status (command output modified)
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.

Feature	Description
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.
Network-Wide Path Insight in Cisco SD-WAN Manager Enhancements	This feature provides enhancements to network-wide path insight tracing, including additional filters and options for traces, DNS domain discovery, and new displays for application flows, trace views, and app trends.
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.
Security Parameters Index in the show crypto ipsec sa Command	This feature qualifies the show crypto ipsec sa command for use in Cisco SD-WAN Manager CLI template and modifies the information displayed about Security Parameters Index (SPI) on the supported routers.
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.
DPI Statistics	This feature lets you view detailed information about the flow of traffic from a device.
Cisco Catalyst SD-WAN Forwarding and QoS	
Per-VPN QoS	When a Cisco IOS XE Catalyst SD-WAN device receives traffic belonging to different VPNs from the branch network, you can configure a QoS policy to limit the bandwidth that can be used by the traffic belonging to each VPN or each group of VPNs.
Cisco Catalyst SD-WAN SNMP	
Support for Cisco Catalyst 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.

Feature	Description
Cisco Catalyst SD-WAN MIBs	The following Cisco Catalyst SD-WAN MIBs are introduced on Cisco IOS XE SD-WAN devices: CISCO-SDWAN-APP-ROUTE-MIB.my CISCO-SDWAN-BFD-MIB.my CISCO-SDWAN-OPER-SYSTEM-MIB.my CISCO-SDWAN-POLICY-MIB.my CISCO-SDWAN-SECURITY-MIB.my
Cisco Catalyst SD-WAN Commands	
show platform software memory	This feature adds support for displaying memory information for specified Cisco Catalyst SD-WAN processes.
NAT Serviceability Enhancement	This feature is used to display configured and operational data specific to NAT.

New and Enhanced Hardware Features

New Features

- Support for UCS-E module—This feature adds a UCS-E template in Cisco SD-WAN Manager for configuring Cisco Unified Computing System (UCS) E-Series servers. For related information, see Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine and Configuring Devices using SD-WAN Manager.

Note Currently, backplane interfaces are not supported for UCS-E module. Only external connectivity is supported.

- Support for Cisco IR1101 Integrated Services Router Rugged—Cisco Catalyst SD-WAN capability can now be enabled on Cisco IR1101 Integrated Services Router Rugged. The following notes apply to this support:
  - Controller devices (Cisco SD-WAN Validator, Cisco SD-WAN Controller, and Cisco SD-WAN Manager) must run Cisco SD-WAN Release 19.2 or later.
  - The default topology is full mesh, but the hub and spoke topology is often used for IoT applications.
  - Cisco Catalyst SD-WAN support on the Cisco IR1101 Integrated Services Router Rugged requires Cisco IOS-XE Catalyst SD-WAN Release 16.12.
  - The Cisco IR1101 Integrated Services Router Rugged has four fixed switch-ports. Make sure to select the correct template.
  - The CLI template is not currently supported.
  - Starting from Cisco IOS-XE Catalyst SD-WAN Release 16.12.1, Cisco IR1101 Integrated Services Router Rugged has dual LTE support with LTE extension module.

- We recommend using up to 50 BFD sessions for scaling.

Important Notes, Known Behavior, and Workaround

- Cisco IOS XE Catalyst SD-WAN devices with the SFP-10G-SR module do not support online insertion and removal (OIR) of this module.
- Cisco vManage Release 20.3.1 implements a hardened security posture to comply with FedRamp guidelines. As a result, your Cisco SD-WAN Analytics login credentials that are stored locally get erased on upgrading the software, and you cannot access the Cisco SD-WAN Analytics 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.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, the **`table`** keyword is added to all show sdwan commands for which the output needs to be displayed in a tabular format. Using **`| tab`** is restricted for all Cisco Catalyst SD-WAN commands starting from Cisco IOS XE Catalyst SD-WAN Release 16.11.x.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.3a, the upgrade considerations are updated for auto-negotiation support. For more information on this, see Upgrade Considerations.

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 IOS XE Catalyst SD-WAN Release 17.6.8a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.8a

Identifier	Headline
CSCwk19970	Cisco IOS XE Catalyst SD-WAN device URLF is unable to detect TLS SNI with "TLS1.3 hybridized Kyber support" enabled on the browser.

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.7

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.7

Identifier	Headline
CSCwd42523	Same label is assigned to different VRFs

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.6a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.6a

Bug ID	Description
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.6

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

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.6

Identifier	Headline
CSCwd45508	Cisco IOS XE Catalyst SD-WAN device does not form BFD across serial link when upgrading from 17.3.3 to 17.6.x
CSCwf61793	Traceback during policy changes.
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail.
CSCwe43341	TLS control-connections down, traffic from control component dropped with SdwanImplicitAclDrop.
CSCwb65396	C1116-4P: cli template push fails with error: 'Error: on line 48: line-mode single-wire line 0'.
CSCwd48781	Cisco IOS XE Catalyst SD-WAN device ASR1k crashed due to critical process cxpd fault.
CSCwf38166	CPP Ucode crash when Multicast traffic and UTD is enabled together on the same Cisco IOS XE Catalyst SD-WAN device.
CSCwf38281	Misprograming during policy changes.
CSCwe58264	TLOC down post IOS XE to Cisco SD-WAN OS Nutella migration when enterprise cert used.
CSCwc68069	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature.
CSCvz79493	AOM pending for OG LKUP handles on MT.
CSCwe04065	The "advertise aggregate" command is lost on device after upgrade.
CSCwe23276	Change in the IPsec integrity parameters breaks the connectivity.
CSCwb90252	Automatically freeing up filesystems stale image or recovered folder (lost+found).
CSCvy53031	Inconsistent behavior found when adding tunnel source config to virtual-template interface.

Identifier	Headline
CSCwd44586	Cisco IOS XE Catalyst SD-WAN device - Login banner config is changed after upgrade to 17.6.3a
CSCwf49597	Traffic is getting dropped with "SdwanDataPolicyDrop" with TunnelReason : MATCHED_NONE.
CSCwe18058	Unexpected reload with IPS configured on 17.6.3a
CSCwe73993	Cisco IOS XE Catalyst SD-WAN device might reload during overlay session entry removal.
CSCwe24567	Cisco IOS XE Catalyst SD-WAN device router happened rebooting suddenly due to ftmd fault.
CSCwe85421	Cisco IOS XE Catalyst SD-WAN device BFD Session Down with interface flap.
CSCwf26771	Invalid L4 Header drop due to multiple encap.
CSCwe64991	Cisco SD-WAN Manager reporting abnormal latency & jitter parameters.
CSCwf95095	Intermittent BFD session flaps on Cisco IOS XE Catalyst SD-WAN device service side interface.
CSCwe15537	Cisco IOS XE Catalyst SD-WAN device : After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.
CSCvy23366	C8300-2N2S + UCSE: Kernel crash on C8300-2N2S with UCSE module.
CSCwe09341	TLOC down post Cisco SD-WAN OS to IOS XE Nutella migration when enterprise cert used.
CSCwe81991	The fugazi crash with qfp-ucode-fugazi in Catalyst 8500L Edge Platform at @posix_mempool_prime_cache.
CSCwe49684	Cisco IOS XE Catalyst SD-WAN device BFD sessions keeps flapping intermittently.

Open Bugs for Cisco IOS XE Release 17.6.6

Identifier	Headline
CSCwe90501	CSR1000v upgrade fails from 17.3.4a to Cisco Catalyst 8000v 17.6.5 due to "advertise aggregate" with vrf.
CSCwj31354	Cisco IOS XE Release 17.6.6 | Template push failure due to service timestamps
CSCwb74384	Cisco IOS XE Catalyst SD-WAN device: confd_cli high CPU utilization after executing "show sdwan app-route stats".
CSCwe70642	AAR overlay actions are applied to DIA traffic.
CSCwf94294	Misprograming during vpn-list change under data policy.

Identifier	Headline
CSCwh39906	Cisco IOS XE Catalyst SD-WAN device: confd_cli may cause high CPU. Parent PID of "confd_cli" containing "show ip fib".
CSCwh37671	The configuration crashed impacting all Cisco IOS XE Catalyst SD-WAN device functionality.
CSCwf43470	Cisco IOS XE Catalyst SD-WAN device : Traceroute not working with NAT pool configuration.
CSCwc19362	Solution : The crash during overnight longevity on Catalyst 8500 Edge Platform (ACE) and ASR1001-HX.
CSCwe27241	The nbar classification error with custom app-aware routing policy.
CSCwh30423	After upgrade of the Cisco Catalyst 8000V to 17.6.4 sometimes template push is failing with error access denied.
CSCvz71647	Optimization of sdwan_process_dp_in and sdwan_process_ dp_out features in cpp dp.
CSCwa19332	Fragmented packets getting dropped unexpectedly when second fragment packet no translate.
CSCwb74821	Cisco IOS XE Catalyst SD-WAN device: unexpected behavior due to unstable power source.
CSCwd20182	[SIT] : When firewall is enabled , speedtest with iperf server configured on vpn 0 fails.
CSCwd71586	The BFD sessions flapping on an interface with SYMNAT may lead to IPSec crash.
CSCwb39206	To Enable VFR CLI in SD-WAN mode.
CSCwf45486	OMP to BGP redistribution leads to incorrect AS_Path installation on chosen next-hop.
CSCwf73123	BFD timers reverting back to default value after negotiating correctly.

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.5a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.5a

Bug ID	Description
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.5

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

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.5

Identifier	Headline
CSCwd47940	Cisco IOS XE Catalyst SD-WAN device: PMTU Discovery is not working after interface flap
CSCwd25368	Cisco IOS XE Catalyst SD-WAN devicePolicyDual: Traffic not getting dropped as per the policy configured
CSCwd12955	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured
CSCwb62474	[SIT] Cisco IOS XE Catalyst SD-WAN device may crash when doing Cisco Catalyst SD-WAN speedtest with WAN flapping
CSCwc23077	Firewall drop seen stating “FirewallL4” seen on Cisco IOS XE Catalyst SD-WAN device
CSCwc79847	Router Crashed | Last reload reason: Critical process ftmd fault on rp_0_0 (rc=134))
CSCwc96444	Cisco IOS XE Catalyst SD-WAN device router is not programming correct next-hop for unicast prefix with multicast config present
CSCwc89328	Cisco IOS XE Catalyst SD-WAN device Might Reboot when vEdge Supporting Explicit IV joins SD-WAN Network
CSCwd06118	IKEv2 Cert-based IPSEC not working between IOS-XE and AWS
CSCwc52538	Cisco Catalyst SD-WAN flows are not distributed and load-balanced evenly and consistently
CSCwd70300	Route-map not getting effect when its applied in OMP for BGP routes (check WORKAROUND in Summary)
CSCwc72569	Template push failed on 17.6.4 with 'service internal' error.
CSCwd45894	Cisco Catalyst SD-WAN ACL TCAM not in sync with configuration
CSCvz96954	17.6: Route-map not getting effect when its applied in OMP for BGP routes
CSCwd34573	Sparrow crashed: fman_fp_image: QFP0.0 CPP Driver LOCKDOWN encountered due to previous fatal error
CSCwc77003	Prefix through hub not intalled in FIB, with OD Tunnels, seeing drops due to FirewallPolicy
CSCwc79145	Throughput degrades when Local TLOC specified in Data Policy goes down
CSCwd14061	FTM is shooting up high and stuck in loop with the function ftm_sa_add().
CSCwd01326	Catalyst 8500L - qfp-ucode-fugazi crashes with SIGABRT within cio infra under heavy load
CSCwd56015	UTD skipped when interface UTD config is used to enable/disable UTD

Identifier	Headline
CSCwc76082	check_sig_ipsec_ike_sessions fails with could not find entry for Tunnel100001
CSCwd15560	With 2 sequences, should not skip if the match is different and action is same
CSCwb85215	Firewall dropping packets in Hub Cisco IOS XE Catalyst SD-WAN device with SIG tunnels
CSCwd11365	Needs cert update - Azure CGW creation fails due to NVA provisioning failure
CSCwd15070	Cisco IOS XE Catalyst SD-WAN device upgrade fails and can't change template due to "advertise aggregate" config w/o prefix-list
CSCwc95218	C8300 with 5G module P-5GS6-GL is losing cellular config at each boot after upgrading to 17.9.1
CSCvz45869	Cisco IOS XE Catalyst SD-WAN device same multicast flow load balanced to different path when AppRoute policy configured
CSCwc28587	C8300 : Crashed without generating any core (Critical process plogd fault on rp_0_0 (rc=75)
CSCwd17381	NAT/DIA traffic is skipping UTD in forward direction after SSNAT path from service-side
CSCwb32635	17.6.2 IOS XE Catalyst SD-WAN - vdaemon file is incomplete when running admin-tech
CSCwc77177	BFD and control packets are dropped when ACL is applied on gigi to which loopback is bind
CSCwd61799	"show utd engine standard logging events" not showing any events
CSCvz20025	SSH connection getting dropped with UTD and Service NAT feature interaction

Open Bugs for Cisco IOS XE Release 17.6.5

Identifier	Headline
CSCvy23366	C8300-2N2S + UCSE: Kernel crash on C8300-2N2S with UCSE module.
CSCwd45508	Cisco IOS XE Catalyst SD-WAN device does not form BFD across Serial link when upgrading from 17.3.3 to 17.6.x
CSCwc68069	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature
CSCwd47937	Device roll back doesn't work on C1121X-8P on 17.6.3a
CSCwd10988	Cisco IOS XE Catalyst SD-WAN device crashes due to OMP process
CSCwc20170	C8500 Cisco IOS XE Catalyst SD-WAN device reloads unexpectedly due to Critical FTMd Fault when VRF Configuration is Pushed

Identifier	Headline
CSCwd79057	Multicast packet loss when Cisco SD-WAN Controllers goes down
CSCwb65396	C1116-4P: cli template push fails with error: 'Error: on line 48: line-mode single-wire line 0'
CSCwd48781	Cisco IOS XE Catalyst SD-WAN device ASR1k crashed due to Critical process cxpd fault
CSCwd76364	Cisco IOS XE Catalyst SD-WAN device crash with imgr_n2_ipsec_sa_ctx_register
CSCwc37465	Unable to push "no-alias" option on static NAT mapping from Management system
CSCwd44586	Cisco SD-WAN Cisco IOS XE Catalyst SD-WAN device - Login banner config is changed after upgrade to 17.6.3a
CSCvz71647	Optimization of Cisco SD-WAN_process_dp_in and Cisco SD-WAN_process_ dp_out features in cpp dp
CSCwb74821	yang-management process confd is not running, controller mode 17.6.2a
CSCwb90252	Automatically freeing up filesystems stale image or recovered folder (lost+found)
CSCwb83236	Traceback: Cisco IOS XE Catalyst SD-WAN device QFP core after pushing data policy with IPv6 interface
CSCwd34941	NAT configuration with no-alias option is not preserved after reload
CSCwd70300	Route-map not getting effect when its applied in OMP for BGP routes (check WORKAROUND in Summary)

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.4

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

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.4

Identifier	Headline
CSCvz93712	VFR is enabled by feature NAT but there is no NAT configured on the interface
CSCwb32059	Cellular interface tracker Down but NAT route persists in the Service VPN Routing Table
CSCwa92082	RG B2B(Box to Box), Interchassis HA, STBY is stuck in STANDBY COLD-BULK on ISR 4461
CSCwb59736	CSR BFD tunnel are zero with Cisco SD-WAN version 17.03.03.0.7
CSCwa00229	Template push failed while deploying C1111-8PLTELA using LTE for ZTP
CSCvz83016	BFD tunnel uptime not showing correct values post upgrade

Identifier	Headline
CSCwb43605	Cisco IOS XE Catalyst SD-WAN device OMPd crash during RIB-out attribute aspath/community processing
CSCwb90470	Cisco IOS XE Catalyst SD-WAN device crashed with last reload reason Critical process cxpd fault.
CSCwb73511	Cisco IOS XE Catalyst SD-WAN device is not able to bring up SIG tunnels after reboot
CSCwa97951	Basic feature template fails on ASR1001-HX with TenGig interface due to negotiation auto
CSCwa67886	UDP based DNS resolution doesn't work with IS-IS EMCP on IOS-XE
CSCvz23982	IOS sending UP Event for the sub interface which is in down state
CSCvx93283	Service Chain is not created when Tracking is disabled
CSCvx18302	[SIT] Speed Test to Internet failing on vEdges and Cisco IOS XE Catalyst SD-WAN devices running 20.3/17.3
CSCvz99832	Cisco IOS XE Catalyst SD-WAN device per class BFD - echo response pkts
CSCwb05743	Crash seen with umbrella config during soak run
CSCwb73664	[SIT] "sh Cisco SD-WAN bfd session" have missing last digit for site-id
CSCwa92137	17.7.1 - Cisco IOS XE Catalyst SD-WAN device is changing ICMP ID in ICMP echo replies intermittently
CSCwa49721	Cisco Catalyst SD-WAN HUB with firewall configured incorrectly dropping return packets when routing between VRFs
CSCwb08636	IPSEC-3-HMAC_ERROR: IPSec SA receives HMAC error seen for TLOCExt setup after upgrade
CSCwb13820	C8Kv crashed at high scale with IPSEC and heavy features configured
CSCwb16723	Traceroute not working on Cisco IOS XE Catalyst SD-WAN device with NAT
CSCwc33311	Cisco IOS XE Catalyst SD-WAN device crash @ imgr_n2_ipsec_sa_ctx_register
CSCwa81471	AOM pending objects with loopbacks binded to tloc-extended interfaces
CSCwc13304	Per-tunnel QoS counters and shapers not working for some bfd tunnel with stale 'nh_overlay' objects
CSCwb71658	[SIT] Traceback seen on ISR4331 and C8300-2N2S-4T2X after enabling ipsec_pwk and reboot
CSCwb76170	IPsec SIG auto tunnels are not coming up
CSCwb91729	Fix mishandling of policy sequence programming failures and notify with syslog/notification

Identifier	Headline
CSCwa30857	Internet SpeedTest with Loopback binding mode doesn't work with implicit ACL drop for return traffic
CSCwa98545	Checks of route leaks creates memory corruption.
CSCwb43423	Cisco IOS XE Catalyst SD-WAN device: IOS XE image installation fails
CSCwc04688	Cisco IOS XE Catalyst SD-WAN device crash observed after enabling NWPI trace with IPv6 traffic
CSCwb78290	Cisco Catalyst SD-WAN-BFD-MIB request gives results intermittently
CSCwb44275	Simulated flows with PPPoE with NAT DIA result in crash consistently
CSCwa57873	Incorrect reload reason - Last reload reason: LocalSoft for Netconf Initiated request
CSCvz37340	The [service timestamps log datetime msec localtime] command cannot be pushed via CLI Addon template
CSCwa25256	Installing new enterprise wan edge cert does not remove old cert causing device to use old cert
CSCwb51595	Missing IOS config (voice translation rule) on upgrade from 17.3 to 17.6
CSCwb40575	After Cisco IOS XE Catalyst SD-WAN device upgrade, umbrella dns config set to NONE in show umbrella config (17.4.2 to 17.6.3)
CSCwb18315	Umbrella DNS security policy doesn't work with Cloud onRamp with SIG tunnels
CSCwb58468	17.8 Sig Autotunnels:tunnel 409 response received
CSCwc04289	Cisco IOS XE Catalyst SD-WAN device: Inconsistency between Path MTU Discovery result and Tunnel MTU
CSCvx74917	[17.5 Umbrella] DNS Packets are not redirected to configured Custom DNS after Umbrella Template Edit
CSCvy34350	Cisco Catalyst SD-WAN gatekeeper optimization for service side nat

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.4

Identifier	Headline
CSCvy23366	C8300-2N2S + UCSE: Kernel crash on C8300-2N2S with UCSE module.
CSCwc32595	BFD sessions remains down if interface flap form up/down/up
CSCwc55260	Cisco Catalyst SD-WAN - Memory leak due to FTMd process
CSCwc38529	[17.6] Traffic seems not inspected by UTD when umbrella is set
CSCwc55467	BFD Tunnel on Cisco SD-WAN router is not staying up, 1 out of 40 tunnels.

Identifier	Headline
CSCwc20170	C8500 Cisco IOS XE Catalyst SD-WAN device Reloads Unexpectedly due to Critical FTMd Fault when VRF Configuration is Pushed
CSCwc54463	Cisco IOS XE Catalyst SD-WAN device C1121x-8P LAN Module is down when high CPU noticed
CSCwb62474	[SIT] Cisco IOS XE Catalyst SD-WAN device may crash when doing Cisco SD-WAN speedtest with WAN flapping
CSCwc37465	Static NAT configuration in CLI with the no-alias keyword cannot be retrieved via NETCONF/YANG
CSCwc52538	Cisco Catalyst SD-WAN flows are not distributed and load-balanced evenly and consistently
CSCwc23077	Firewall drop seen stating “FirewallL4” seen on Cisco IOS XE Catalyst SD-WAN device
CSCwb83236	Traceback: Cisco IOS XE Catalyst SD-WAN device QFP core after pushing data policy with IPv6 interface
CSCwc53885	IOS-XE "no ip nat" config is allowed to be committed and removes nat routes among other nat config
CSCwc59650	show Cisco SD-WAN app-fwd cflowd flows vpn X format tabled does not show all flows for vpn X
CSCwb74821	Yang-management process confd is not running, controller mode 17.6.2a
CSCwc42978	ISR1100-4G looses all BFD sessions with Invalid SPI
CSCwc27208	BFD sessions not coming UP because of ANTI-REPLAY-FAILURES

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.3a

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

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.3a

Bug ID	Description
CSCvw68560	17.5: OMP is advertising unfiltered ipv6 routes from BGP
CSCvz37661	17.6 to 17.7 : Continuous 4461 Octeon crypto crash. does not stay up.
CSCvz40222	SDRA : RA headend crash with Critical process vdaemon fault with tunnel flaps
CSCwa52915	Replicator with direct multicast source reachability should be preferred among selected replicators
CSCvx40516	17.5 ZBFW + NAT: Traffic flow In2Out scenario failed

Bug ID	Description
CSCwa26509	Shut/no shut of endpoint-tracker attached tunnel, doesn't create probe again on 17.6.2
CSCvz99404	Cisco Catalyst SD-WAN ImplicitAclDrop seen on non Cisco Catalyst SD-WAN interface after upgrade to 17.6.1
CSCwa12878	Cisco SD-WAN Manager intermittent netconf connection issue to Cisco IOS XE Catalyst SD-WAN device
CSCwa98047	SASE - after Cisco IOS XE Catalyst SD-WAN device upgrade, umbrella dns config set to NONE in show umbrella config
CSCwa42747	Fugazi and TSN get crashed consistently when start nwpi trace
CSCwa04960	[SIT] OMPD process memory leak seen on Cisco IOS XE Catalyst SD-WAN device
CSCwa83899	Cisco SD-WAN Manager getting "non-ok device" error when attaching a template to several devices.
CSCvz74773	Discrepancies in CLI and GUI interface details (Truncating interface numbers)
CSCvz62032	Attach gateways failed in cloud express
CSCvz87855	mroute state stuck after Cisco IOS XE Catalyst SD-WAN device failure is restored
CSCvz69103	Pending obejcts and download failure with policy update from 17.7.1 throttle image
CSCwa73783	Incorrect Cisco IOS XE Catalyst SD-WAN device COR for SAAS Policy Sequence Programming
CSCwa19074	Infinite output from command show Cisco Catalyst SD-WAN tunnel sla
CSCwa34783	BFD session get stuck to down after site to site speedtest with Loopback as WAN + NAT
CSCwa92411	Slowness issues casued by intermittent traffic drop on ISRv ingress from GRE tunnel
CSCwa64990	Cisco Catalyst SD-WAN NAT DIA with data policy not work properly with static destination NAT
CSCvv82985	dhcpv6_relay:dhcp-client on branch not receive ipv6 address
CSCwa78762	Umbrella SIG tunnel creation failed after config reset for PnP
CSCvz81428	SIT : vedaemon assert noticed in the ISR 4221 over weekend longevity
CSCwa93930	"Alarms alarm bfd-state-change syslog" command is getting rejected while reconfiguring the device.
CSCwa96768	SIP/ICMP flow can't be forwarded after FEC enabled and WAN link re-connected.
CSCwa71862	Crash may be hit when start stop flow monitor in NWPI domain monitor
CSCvz41647	Partial multicast drops are seen after a failover event in a site with two Cisco IOS XE Catalyst SD-WAN devices

Bug ID	Description
CSCwa45487	DNS packets gets injected improperly with sdwan system ip and dropped from Service VPN
CSCwb07025	Packets are being fragmented even if Dont Fragment is set.
CSCwa53223	Cisco IOS XE Catalyst SD-WAN device app-route policy not load balancing traffic as expected when SLA doesn't meet
CSCwa78020	ZBFW dropping packets as Input VPN ID set to 0 instead of 99. SDWAN VPN : 99

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.3a

Identifier	Headline
CSCvz93712	VFR is enabled by feature NAT but there is no NAT configured on the interface
CSCwb52616	Cisco IOS XE Catalyst SD-WAN device doesn't inject ping packets due to no route although data policy has nat vpn-0
CSCwa92082	RG B2B(Box to Box), Interchassis HA, STBY is stuck in STANDBY COLD-BULK on ISR 4461
CSCwb03455	Inter-vrf route leaking not working and packet drop seen due to IPv4 Unclassified
CSCvz83016	BFD tunnel uptime not showing correct values post upgrade
CSCwa67886	UDP based DNS resolution doesn't work with IS-IS EMCP on Cisco IOS XE Catalyst SD-WAN device
CSCwb42807	After Enforce Software Version (ZTP) completed successfully, it automatically rolled-back
CSCwb05743	Crash seen with umbrella config during soak run
CSCwb43423	Cisco IOS XE Catalyst SD-WAN device: IOS XE image installation fails
CSCwa92137	Cisco IOS XE Catalyst SD-WAN device is changing ICMP ID in ICMP echo replies intermittently
CSCwa49721	Cisco Catalyst SD-WAN HUB with firewall configured incorrectly dropping return packets when routing between VRFs
CSCwb18223	SNMP v2 community name encryption problem
CSCwb16723	Traceroute not working on Cisco IOS XE Catalyst SD-WAN device with NAT
CSCwa81471	AOM pending objects with loopbacks binded to tloc-extended interfaces
CSCwa11349	ASR1002-HX High QFP Utilization
CSCwa64993	CXP for SaaS takes more than 5 min to detect indirect path failure over TLOC-extension
CSCwa98545	Checks of route leaks creates memory corruption.

Identifier	Headline
CSCvy23366	C8300-2N2S + UCSE: Kernel crash on C8300-2N2S with UCSE module.
CSCwb33625	Cisco SD-WAN Manager:Speed Test Not working for ISR1100-4g and C8300 devices
CSCwb32635	17.6.2 Cisco IOS XE Catalyst SD-WAN device - vdaemon file is incomplete when running admin-tech
CSCvx74917	[17.5 Umbrella] DNS Packets are not redirected to configured Custom DNS after Umbrella Template Edit
CSCwb51595	Missing IOS config (voice translation rule) on upgrade from 17.3 to 17.6
CSCwb18315	Umbrella DNS security policy doesn't work with Cloud onRamp
CSCwa68540	FTP data traffic broken when UTD IPS enabled in both service VPN

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.2

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

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.2

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	SD-WAN policy is not correctly programmed in Cisco IOS XE Catalyst SD-WAN device
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

Bug ID	Description
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 SD-WAN 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"
CSCvz86972	Cisco IOS XE Catalyst SD-WAN DST Root CA X3 Expiration causing umbrella integration to fail
CSCvz09460	Remote Server: Dont send userid and password in download notifications
CSCvy78170	SIT : The cpu usage percentage is shown incorrect in the Cisco SD-WAN Manager-alarms
CSCvz74825	Crash may be hit when start stop flow monitor in NWPI domain monitor
CSCvz31429	fman_fp crash while running stress test
CSCwa11628	Umbrella Certificate is not getting copied to HW device causing umbrella integration to fail
CSCvz07713	ASR1001HX crashed when enable fair-queue under class-default of per-Tunnel QoS policy template
CSCvz76008	C8300 router might get crashed during config update with flow-visibility and flow-visibility-ipv6
CSCvz14059	more than 4 unique sla policies applied to Cisco IOS XE Catalyst SD-WAN device.
CSCwa03524	Fugazi crash @posix_burst_add_pkt_slow with 4K SDWAN tunnels

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.2

Bug ID	Description
CSCwa14435	Cisco IOS XE Catalyst SD-WAN device | tcp adjust mss not working for incoming TCP packets
CSCvz93712	VFR is enabled by feature NAT but there is no NAT configured on the interface
CSCwa08336	Cloud SaaS packets does not follow the best performing path
CSCvz41647	Partial multicast drops are seen after a failover event in a site with two Cisco IOS XE Catalyst SD-WAN devices
CSCwa08713	Multicast traffic is getting dropped due to SdwanDataPolicyDrop
CSCwa11291	QOS stats showing all traffic in queue 2
CSCvy83781	Infinite output from command show sdwan tunnel sla
CSCwa11349	ASR1002-HX High QFP Utilization
CSCvz79855	CPU spike is observed on GD performance when Adaptive FEC is enabled
CSCvz99404	SdwanImplicitAclDrop seen on non-SDWAN interface after upgrade to 17.6.1
CSCvz62032	Attach gateways failed in cloud express
CSCwa14636	Cisco IOS XE Catalyst SD-WAN device stopped forwarding traffic. Suspect OMPd is busy
CSCvz91487	Cisco IOS XE Catalyst SD-WAN device config changed via CLI while control is down don't revert once the control is restored
CSCwa19074	Infinite output from command show sdwan tunnel sla
CSCwa22412	ftmd crash during reload
CSCwa22254	uniterested traffic getting dropped due to natout2in feature when fragmented
CSCwd42523	Same label is assigned to different VRFs

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

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

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

Bug ID	Description
CSCvq11402	[SSL-Proxy-Policy] Webroot - url cloud lookup timeout is 60s (way too long to hold the traffic)
CSCvw88366	data traffic failing in SIG + firewall config

Bug ID	Description
CSCvx45788	cannot apply ciscoCisco Catalyst SD-WAN.cfg due to vpg-log-server-acl ACL on VirtualPortGroup0 for logging
CSCvx49311	Cisco Catalyst SD-WAN Manager pushing invalid "no shutdown" command to ISR Service-Engine interface
CSCvx53399	fman_fp_image crashed with ZBFW config change
CSCvx57615	ZBFW blocking ACK packets for applications using cloudexpress SaaS set to use a Gateway with synsent
CSCvx58099	C8500-12X4QC does not send logs to Cisco Catalyst SD-WAN Manager when harddisk is not installed
CSCvx59899	ISR4431/K9 rebooting due to CPP crashing becaue of UTD feature.
CSCvx60842	OnDemand Tunnel- Site-ID doesnt update after change it
CSCvx72232	rbuf-ooh crash in HSL
CSCvx79113	Cisco Catalyst SD-WAN Cisco IOS XE Catalyst SD-WAN device : traffic simulation tool shows traffic blackhole
CSCvx88246	Packets dropped due to firewall + data policy interop issue
CSCvy00963	On Cisco Catalyst SD-WAN Manager 20.4.1, traceroute on Cisco IOS XE Catalyst SD-WAN device leads to outage at the site
CSCvy03584	Cisco IOS XE Catalyst SD-WAN device fails to capture Cisco Catalyst SD-WAN-related outputs to admin-tech
CSCvy06736	Config out of sync after upgrading to 17.4.1
CSCvy09343	CFM inject packet is not marked as high priority
CSCvy09777	Cisco IOS XE Catalyst SD-WAN device running 17.4.1b crashing with NAT Backtraces everytime we shut no-shut PPPoE
CSCvy13261	ASR1001-X is not tagging BGP prefixes with OMP tags
CSCvy13735	BFD tunnels stuck in down state after port-hop
CSCvy14126	ISR4331 are crashing frequently 17.4.1b
CSCvy33007	"Best of Worst" Fallback mode causes reachability issue when routes flap
CSCvy35044	Signature update failure - SSL-CERTIFICATE_VERIFY_FAILED
CSCvy37216	Cisco Catalyst SD-WAN Manager fails to push template - interface config stuck
CSCvy44563	cpp-mcplo-ucode crash due to stuck thread with extranet route leaking between vpns
CSCvy45478	Device is showing the passwords in clear text rather than hash

Bug ID	Description
CSCvy47279	C1111 device crashed when PPPoE(running NAT) cable pulled out
CSCvy52761	adding multilink frame relay sub-interface to Cisco Catalyst SD-WAN fails; "Aborted: application error"
CSCvy54314	Data-policy local-tloc with app-route is dropping packets when SLA is not met
CSCvy55507	Cisco IOS XE Catalyst SD-WAN devices are dropping incoming GRe keepalives due to implicit ACL
CSCvy58266	vDaemon crashes due to buffer overflow with read/write in TAM
CSCvy64180	Cisco IOS XE Catalyst SD-WAN device C1121-4P crahed with Localsoft error
CSCvy78123	Cisco IOS XE Catalyst SD-WAN device: High CPU usage due to Multicast and Data Policy configuration.
CSCvy93830	BFD tunnel uptime not showing correct values post upgrade to 17.6.01
CSCvy98015	Cisco IOS XE Catalyst SD-WAN device(UTD) : ICMP time Exceed packet dropped on UTD by 'Err: unwanted error messages'
CSCvx36167	MT-SIT: Template attach failed with "Server error: lte modem syntax error: element does not exist"
CSCvw68402	Template push to Cisco IOS XE Catalyst SD-WAN device fails when changing system-ip due to Cisco Cisco SD-WAN controller centralized policy

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

Bug ID	Description
CSCvx17563	ISR4331/K9 running 16.12.04 crashed with Segmentation fault(11), Process = Cellular CNM
CSCvx42400	Cisco IOS XE Catalyst SD-WAN device Experiences Unexpected reboot with: Last reload reason: Critical software exception
CSCvx44834	ASR1K - ACE entry added after object-group is missing in hardware causing packets drops
CSCvy33818	On MTT Cisco SD-WAN Manager system IP persists after invalidating and deleting the edge devices.
CSCvy55408	C1121 router multiple crash. - session hash corrupted
CSCvy72970	Active ftp not working with UTD+HTX for security and Unified policy.
CSCvy78501	17.6: AAR not working properly as configured SLA classes are not shown under app-route stats

Bug ID	Description
CSCvy79833	Cisco IOS XE Catalyst SD-WAN device: Cellular related AOM pending objects after IOS-XE upgrade
CSCvy83674	Cisco Catalyst 8200: Observing low performance compare to UP performance numbers
CSCvy86497	BFD session flap/down while control connection with Cisco SD-WAN Manager is going down
CSCvy98784	AppQoE DP stats for active connections shows huge bogus value
CSCvz08674	Cisco IOS XE Catalyst SD-WAN device rebooted 2 time with CPP 0 failure Stuck Thread
CSCvz08945	low-bandwidth-link doesn't reduce number of BFD packets
CSCvz11158	Not able to upgrade Cisco IOS XE Catalyst SD-WAN device from Cisco SD-WAN Manager | from 16.12.3 to 17.3.3
CSCvz24199	cEdge: Transport interface IP is unexpectedly NATed to pool address in DIA scenarion
CSCvz25403	NetApp: Issues with traffic does not get forwarded via TLOC extended interface
CSCvz30626	20.6: Cisco SD-WAN Manager Main Dashboard , with Top Application Data => SSL proxy, data is empty
CSCvz33108	After uploading the serial file list to the Cisco SD-WAN Manager, the edges lost Control Con. and BFD sessions
CSCvz35967	cEdge reboot due to "Critical process fman_fp_image fault on fp_0_0 (rc=134)"
CSCvz37551	Switchport Feature Template is unable to create VLANs- Missing VLANs on VLAN-DATA BASE
CSCvz40788	Cisco Catalyst SD-WAN tunnels are not coming up in Multilink Frame relay sub-interface
CSCvz38312	ISR1100 - cedge: Tx queue hang issue on RJ45 ports
CSCvz62602	Extranet local switch crash when mdata is 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.

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

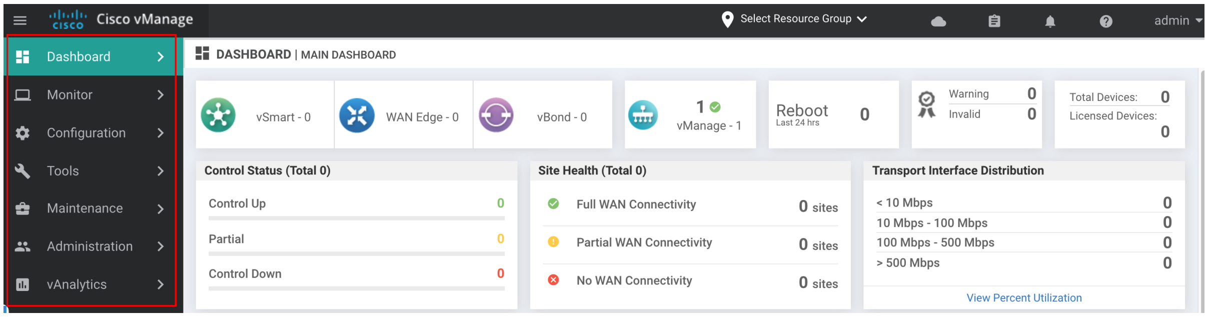


Figure 2: Navigation Menu (Collapsed) in Cisco vManage Release 20.6.1 and Later

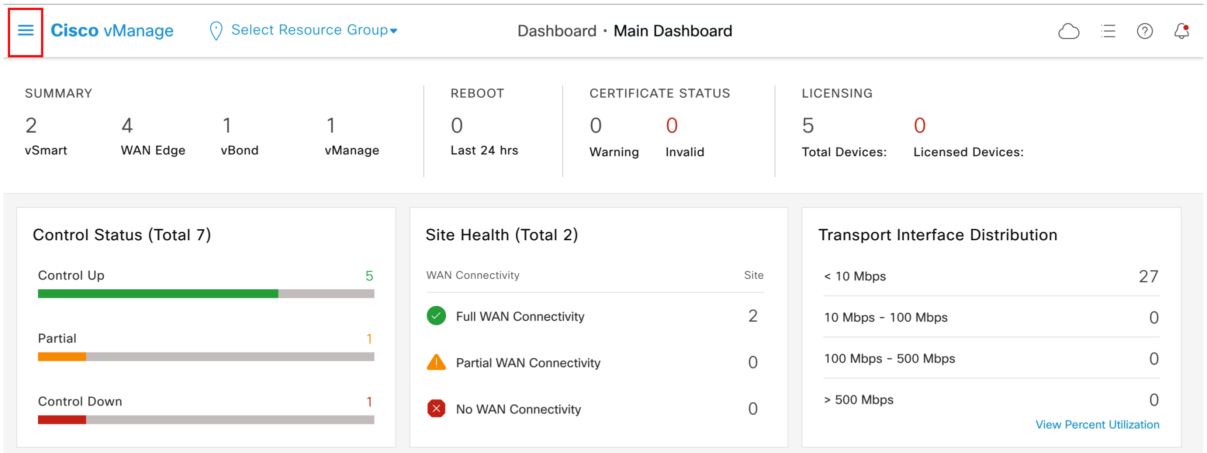
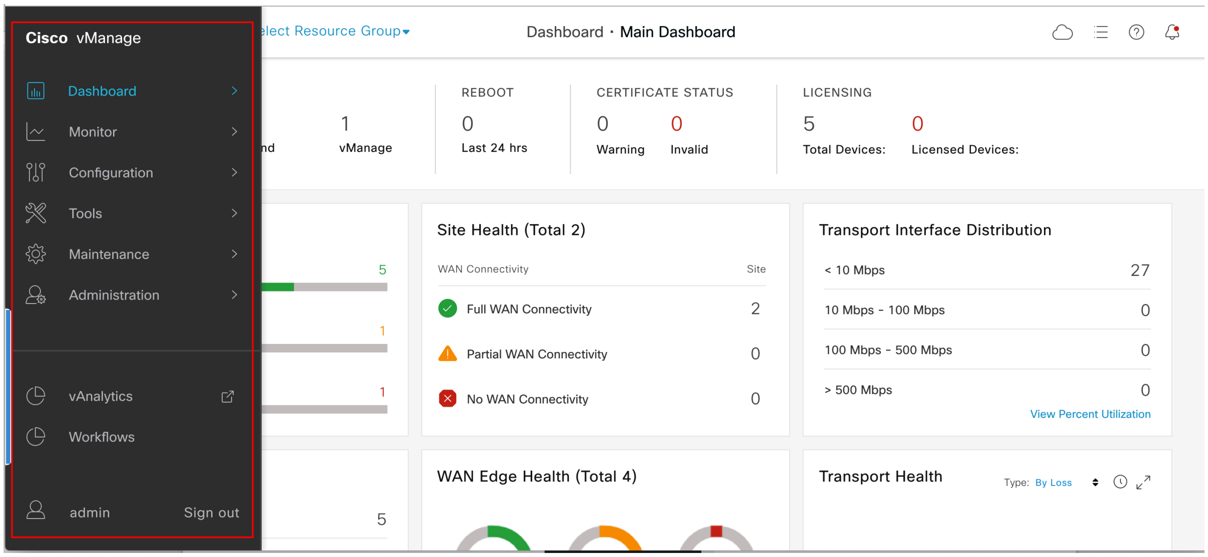


Figure 3: Navigation Menu (Expanded) in Cisco vManage Release 20.6.1 and Later



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

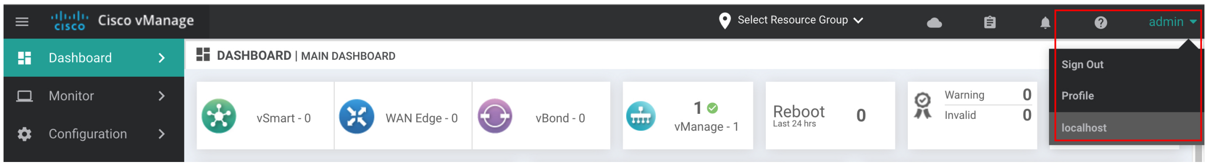
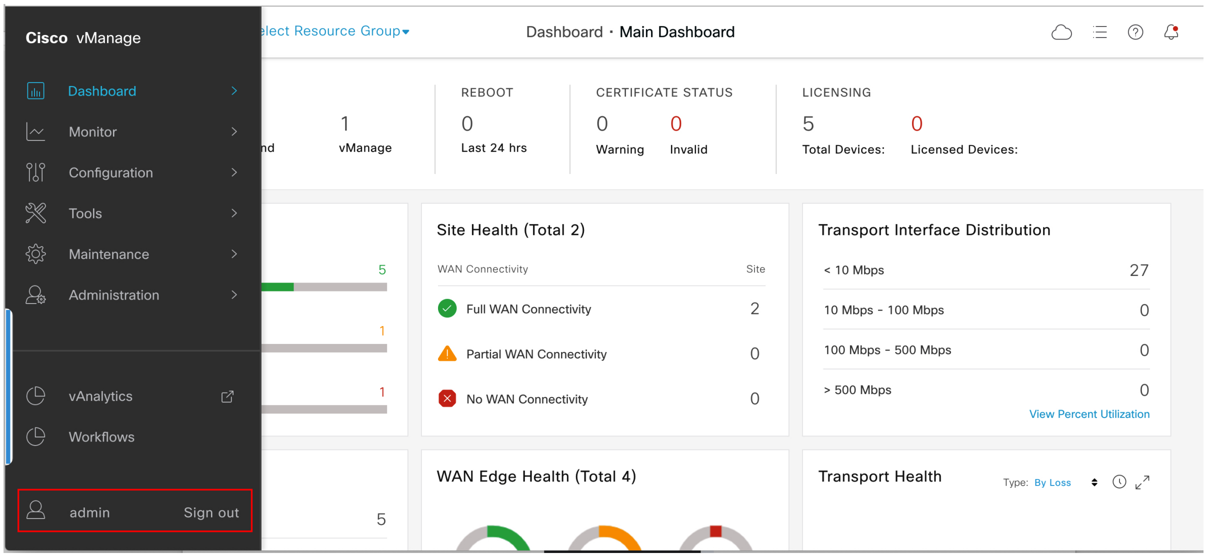


Figure 5: User Profile and Sign Out Options in Cisco vManage Release 20.6.1 and Later



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

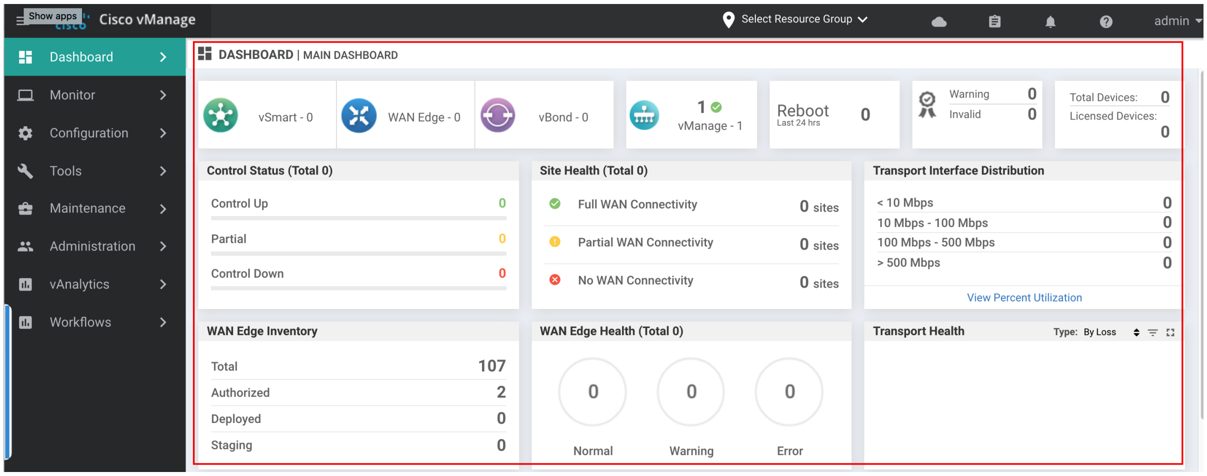
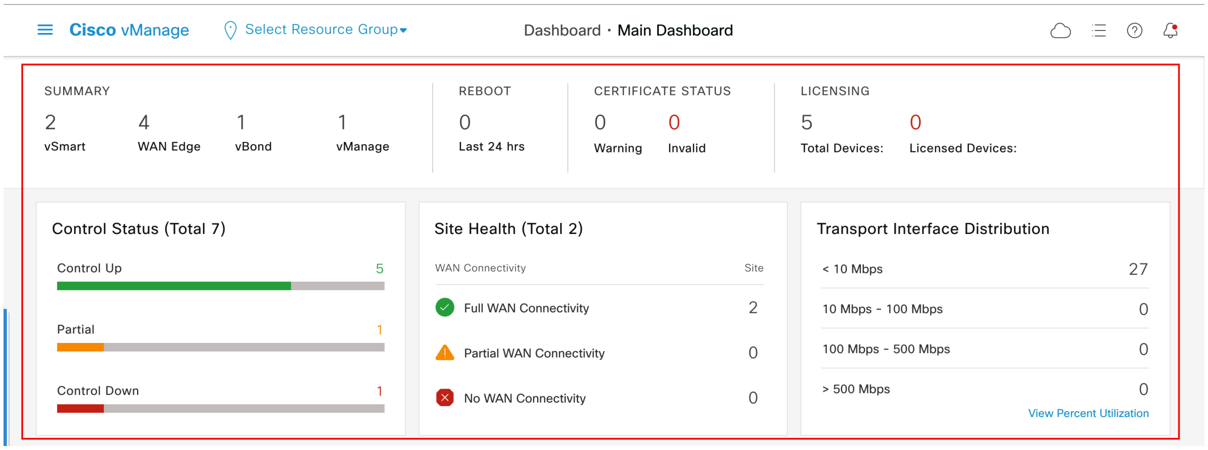


Figure 7: Main Dashboard in Cisco vManage Release 20.6.1 and Later



SUMMARY

2 vSmart

4 WAN Edge

1 vBond

1 vManage

REBOOT

0 Last 24 hrs

CERTIFICATE STATUS

0 Warning

0 Invalid

LICENSING

5 Total Devices:

0 Licensed Devices:

Control Status (Total 7)

Control Up	5
Partial	1
Control Down	1

Site Health (Total 2)

WAN Connectivity	Site
Full WAN Connectivity	2
Partial WAN Connectivity	0
No WAN Connectivity	0

Transport Interface Distribution

< 10 Mbps	27
10 Mbps - 100 Mbps	0
100 Mbps - 500 Mbps	0
> 500 Mbps	0

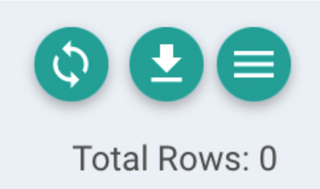
View Percent Utilization

Other Changes

The redesign includes:

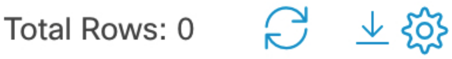
- New icons across Cisco SD-WAN Manager

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

  Total Rows: 0

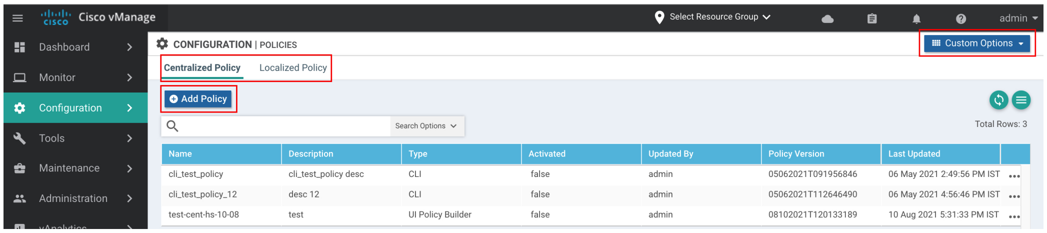
  Figure 9: Example of Icons in Cisco vManage Release 20.6.1 and Later

  Total Rows: 0

- 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

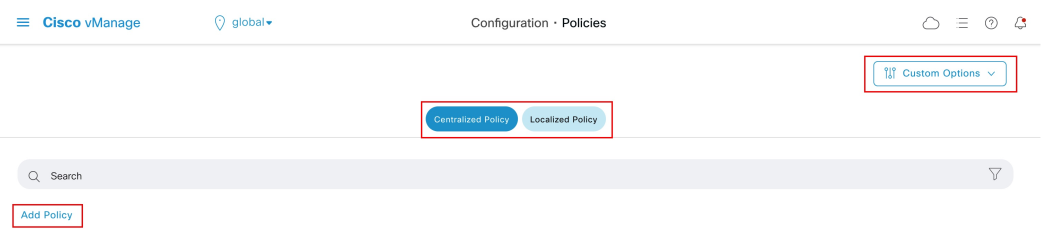
  

CONFIGURATION | POLICIES

Total Rows: 3

Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
cli_test_policy	cli_test_policy desc	CLI	false	admin	05062021T091956846	06 May 2021 2:49:56 PM IST
cli_test_policy_12	desc 12	CLI	false	admin	05062021T112646490	06 May 2021 4:56:46 PM IST
test-cent-hs-10-08	test	UI Policy Builder	false	admin	08102021T120133189	10 Aug 2021 5:31:33 PM IST

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

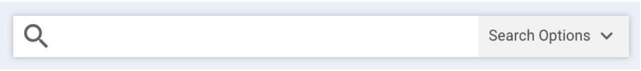
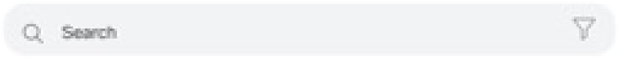


Figure 13: Example of Search Bar in Cisco vManage Release 20.6.1 and Later



Related Documentation

- Release Notes for Previous Releases
- Software Installation and Upgrade for Cisco IOS XE Routers
- 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.