Release Notes for Cisco Catalyst SD-WAN Control Components Release 20.6.x

First Published: 2021-10-16

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
- 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 Catalyst SD-WAN Control Components 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 Control Components, 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 SD-WAN Manager.

Related Releases

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

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

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

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.

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.

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.

Feature	Description
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 17.6.1a

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.
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.

Feature	Description
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.
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.

Feature	Description
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 ISR 1000 series 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	
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.

Feature	Description
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.

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

This section applies to Cisco vEdge devices.

Table 3: 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.
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 4: 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.

Feature	Description
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.
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	

Feature	Description
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	
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

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.
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.
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

- If your ConfigDB (Neo4j) username contains a – (hyphen), the ConfigDB upgrade fails. For example, db-admin. Remove the hyphen before you upgrade the ConfigDB.
- The Cisco SD-WAN vManage 20.6.3 release is impacted by the following defect, CSCwc15033 ,which may affect your use of Cisco SD-WAN Manager software. We strongly recommend you to upgrade your Cisco vManage to the recommended Cisco vManage Release 20.6.3.1 or later to resolve this issue. For more information see, Cisco SD-WAN Release 20.6.3 Software Advisory Notice.
- In Cisco vManage Release 20.5.x and earlier releases, if you created a template with the encrypted data field, the template push fails in Cisco vManage Release 20.6.x. The template push fails due to the change in the encryption library of Cisco vManage Release 20.6.x, and the following error message displays: **Bad ciphertext padding provided**. To successfully push template on the device, update and resave the template.
- Starting from Cisco SD-WAN Release 20.4.1.1, Microsoft Azure environment is supported for deploying CCisco SD-WAN Control Components (Cisco SD-WAN Validator, Cisco SD-WAN Controller, and

Cisco SD-WAN Manager). The support is limited to Cisco Catalyst SD-WAN cloud-based deployments only.

- If SD-AVC is enabled using Cloud Connector or custom applications while upgrading from Cisco vManage Release 20.3.1 to Cisco vManage Release 20.6.1 and later releases, during the upgrade, a defect CSCwd35357 is impacting the data plane. We strongly recommend you to contact the Cisco TAC to perform a workaround while upgrading.
- If you upgrade Cisco vManage from Cisco vManage Release 20.3.1 to Cisco vManage Release 20.6.1, the **Data Stream** settings found in **Cisco SD-WAN Manager Menu** > **Administration** > **Settings** is auto-disabled. Enable the **Data Stream** settings once again post upgrading to Cisco vManage Release 20.6.1.
- If your Cisco SD-WAN Manager is running Cisco vManage Release 20.6.1 and your Cisco vEdge devices are running Cisco SD-WAN Release 20.3.x, a defect CSCwc64459 prevents Cisco SD-WAN Manager from pushing the device templates as expected.
- Cisco SD-WAN Control Components Release 20.6.5 is impacted by the defects CSCwb89273 and CSCwd94839 and impacts the performance of Cisco SD-WAN Manager. We recommend you to upgrade to Cisco Catalyst SD-WAN Control Components Release 20.6.5.1.
- Cisco SD-WAN Control Components Release 20.6.x is impacted by the defect CSCwf75979 and exposed your Cisco SD-WAN Manager to a vulnerability. We recommend you to updgrade to Cisco Catalyst SD-WAN Control Components Release 20.6.6.
- For existing Cisco CSR 1000V deployments: Upgrade Cisco SD-WAN Manager to Release 20.9.5 or later, then upgrade the CSR 1000V to Catalyst 8000V to continue using Cisco virtual devices as the Interconnect Gateway in the Equinix Fabric.

  For more information, see Cisco SD-WAN Manager Upgrade Paths.

Cisco SD-WAN Manager Upgrade Paths

For information about Cisco SD-WAN Manager upgrade procedure, see Upgrade Cisco vManage Cluster.

Starting Cisco SD-WAN Manager Version	Destination Version					
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x
18.x/19.2.x	Direct Upgrade	Direct Upgrade		Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x

Starting Cisco SD-WAN Manager Version	Destination Version					
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x
			Check disk space* • If the disk space is more than 2GB: Direct Upgrade • If the disk space is less than 2GB: Step upgrade through 20.1 • If you are upgrading to 20.3.5, the available disk space should be at least 2.5 GB. For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to			

Starting Cisco SD-WAN Manager Version	Destination Version					
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x
			5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.			
20.1.x	Not Supported	Direct Upgrade	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade through 20.3.x	Step upgrade through 20.3.x

Starting Cisco SD-WAN Manager Version	Destination Version					
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x
20.3.x	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version					
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x
20.4.x	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.
20.5.x	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade

*To check the free disk space using CLI,

1. Use the vshell command to switch to vshell.
2. In vshell, use the df -kh | grep boot command.

**Cluster upgrade must be performed using CLI

- Use the following command to upgrade the configuration database. This must be done on only one node in the cluster:

```
request nms configuration-db upgrade
```

Note We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

- Enter login credentials, if prompted. Login credentials are prompted if all Cisco SD-WAN Manager server establish control connection with each other. After a successful upgrade, all configuration-db services are UP across the cluster and the application-server is started.

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 Catalyst SD-WAN Control Components Release 20.6.8

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.8

Identifier	Headline
CSCwe75148	"valid-vedges" list on Cisco SD-WAN Validator/Cisco SD-WAN Controller get empty, leading to control connection down when rebooted.
CSCwk43942	Cisco SD-WAN Manager software cross-site scripting vulnerability.

Bugs for Cisco Catalyst SD-WAN Control Components 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 Catalyst SD-WAN Control Components Release 20.6.7

Identifier	Headline
CSCwi03952	Cisco SD-WAN Manager Template push failure | Failed to update configuration - CLI generation failed.
CSCwh18874	Replication takes 4+ hours to inject the 100MB of data on standby cluster-No Make Primary to switch.
CSCwh93441	[Cisco SD-WAN Manager Unable to login SSH including ciscotacro/ciscotacrw.
CSCwf98777	Cisco SD-WAN Manager policy is not sending the updated tloc information.

Identifier	Headline
CSCwi04802	Create CGW failing with "Public access is not permitted on this storage account".
CSCwi30235	Issue with accessing Cisco SD-WAN Manager 20.6.6 GUI using upper-case letter on TACACS username.
CSCvx00337	Cisco SD-WAN Manager - Wildfly allocation reduced after upgrade.
CSCwd16027	Unable to generate report from Cisco SD-WAN Manager for SLP Offline mode - Error occurred while generating report.
CSCwi27589	Cloud on ramp for multicloud deploy fails with error : Azure Error: RequestDisallowedByPolicy
CSCwh28301	Cisco SD-WAN Manager GUI becomes very slow when a large template.
CSCwc05127	Breakdown of U-Plane communication after updating Cisco SD-WAN Controller CiscoPKI certificate.
CSCwd69360	SIG feature template will not retain tunnel destination modified variable names Cisco SD-WAN Manager 20.6.4
CSCwh18738	Licenses unapplied from License Management in Cisco SD-WAN Manager after DR failover/failback.
CSCwf95317	Devices are not receiving the preference via the policy in a Multi-Tenant environment.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.6

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.6

Identifier	Headline
CSCwb08600	Missing hostname in some alarms.
CSCwf68955	Cisco SD-WAN Manager Log Poisoning bypass
CSCwf68959	Cisco SD-WAN Manager Audit Log CSV payload injection
CSCwf75979	Cisco SD-WAN Manager Local File Inclusion Vulnerability
CSCwc08313	System does not throw an error message for the overlapping policies in some cases.
CSCwc43513	The stats are not getting processed on Cisco SD-WAN Manager GUI running 20.8.1 code
CSCvz97023	Cisco SD-WAN Manager/Cisco SD-WAN Controller is not forming control connection with newly added Cisco SD-WAN Validator.
CSCwe34379	Cisco SD-WAN Manager access failed when accessing Cisco SD-WAN Manager using DNS record.
CSCwd94839	Cisco SD-WAN Manager GUI becomes unavailable due to authentication errors against configuration-db.

Identifier	Headline
CSCwe14017	20.6.5 Cisco SD-WAN Manager and Cisco SD-WAN Controller upgrade fail via Cisco SD-WAN Manager UI.
CSCwd94301	MTT correlation engine not generating OMP Alarms from OMP Event received from Cisco SD-WAN Controller.
CSCwe32116	Cisco SD-WAN Manager : DSPFarm template error "Duplicate value:mediaresourcegroupname".
CSCvx00337	Cisco SD-WAN Manager- Wildfly allocation reduced after upgrade.
CSCvu76345	Class-map mapping issue for forward-class with QoS map and centralized policy.
CSCwc65025	Email notifications failing when security is set as TLS with Gmail SMTP.
CSCwb38461	Can't get licenses from licensing portal to Cisco SD-WAN Manager.
CSCwd60889	CPU average values reported to Cisco SD-WAN Manager are incorrect.
CSCwb43140	The java.lang.OutOfMemoryError: unable to create native thread (may lead to sysmgr got signal 11 crash)
CSCwf03555	Cisco SD-WAN Manager unable to parse certain time zones and is triggering certificate installation process.
CSCwc47669	Cisco SD-WAN Manager cannot edit ZBFW policy.
CSCvz92332	Cisco SD-WAN Manager not saving "Smart Account Credentials" in **Administration** > **gt** > **Settings**.
CSCwd54278	The aaamgr process restarts unexpectedly.
CSCwf09036	Cisco SD-WAN Manager configures incorrect IKEv2 lifetime for IPSec tunnels.
CSCvt47226	Routes missing on a Cisco Catalyst SD-WAN Edge devices in a graceful-restart scenario.
CSCwd37096	Enabled usage but prepaid consumption - Product instance "UDI_PID: Cisco SD-WAN Manager.
CSCwf49674	Cisco SD-WAN Manager is modifying load_balance .json leading to the edges to be disconnected.
CSCwf28362	Cisco SD-WAN Manager is not generating alarm notifications to be sent to Webhooks server.
CSCvz88483	Template push failure because of error: Failed to publish the task on message bus.
CSCwf75979	Cisco SD-WAN Manager local file inclusion vulnerability.
CSCwd46383	Cisco Catalyst SD-WAN Software Denial of Service Vulnerability

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.6

Identifier	Headline
CSCwh22627	IDP users shows: Invalid response the status code is missing in the response from server.
CSCwh44411	Cisco SD-WAN Manager application-server diagnostics is not displaying disk I/O statistics for Cisco SD-WAN Manager storage.
CSCwh29973	MTT: Sync issue between primary and standby cluster nodes pertaining to templates for multi-tenants.
CSCwh42650	"All BGP peering sessions are down" alarm gets triggered for no apparent reason.
CSCwf94302	New instances on cloud came up with duplicate chassis number.
CSCwf07155	"Set CSR Properties" for Controll Component Certifdication Authentication setting on Cisco SD-WAN Manager GUI is not getting disabled.
CSCwh32780	Cisco SD-WAN Manager cluster - neo4j needs hardcoded heap memory size in large deployments.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5.5

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5.5

Identifier	Headline
CSCwf76218	Cisco SD-WAN Manager Unauthenticated REST API Access Vulnerability.
CSCwf82344	Cisco SD-WAN Manager Unauthenticated REST API Access Vulnerability.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.4.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.4.2

Identifier	Headline
CSCwf76218	Cisco SD-WAN Manager Unauthenticated REST API Access Vulnerability.
CSCwf82344	Cisco SD-WAN Manager Unauthenticated REST API Access Vulnerability.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.3.4

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.3.4

Identifier	Headline
CSCwf76218	Cisco SD-WAN Manager Unauthenticated REST API Access Vulnerability.
CSCwf82344	Cisco SD-WAN Manager Unauthenticated REST API Access Vulnerability.

Identifier	Headline
CSCwf68936	Cisco SD-WAN Manager Authorization Bypass Vulnerability
CSCwf55823	Cisco Catalyst SD-WAN Manager Authorization Bypass Vulnerability

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5.4

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5.4

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

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5.3

Resolved Bugs for Cisco Catalyst SD-WAN Control Components 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 Cisco SD-WAN Manager
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
CSCwf28118	Cisco vEdge: Certificate issue on Cisco vEdge devices

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.3.3

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.3.3

Identifier	Headline
CSCwa60525	Device template fails due to community string error after upgrade to 20.6
CSCwc41119	Duplicate Role descriptors found in IDP metadata
CSCwb35787	20.4 TACACS: old password working after password change on TACACS server
CSCwb13243	Can't update BGP template :"RangeError: Maximum call stack size exceeded"

Identifier	Headline
CSCvz91492	Browser freezes and CPU hits 100 while updating configuration template on vManage.
CSCwc04446	Default route is not installed in the routing table of VPN 0 if the VNIC is changed in OpenStack
CSCwa09345	Cisco SD-WAN Manager GUI crashes when enabling CloudOnRamp for SaaS Application List
CSCwb28681	Updating resource group name does not remove the old name in the CLI
CSCwc81937	Cisco SD-WAN Manager has extra Netconf Sessions when making API calls
CSCwb11588	THe 20.4.2 Cluster vManage Dashboard discrepancy. CLI vs the GUI in the Site Health column
CSCwb62862	Cisco vSmart OMP peerings flap with devices when taking admin tech on all Cisco vSmarts
CSCwa87012	The route policy to match multiple community string, Cisco SD-WAN Manager does not generate match community command
CSCwc00863	The OMPD crash on policy update
CSCvz35603	The VRRP optional fields Server error
CSCwb38187	Cisco SD-WAN Manager - 20.6.2.1 template push failed due to optional field - Invalid value for prefix
CSCwb59024	The all stat-db settings except DPI is not available after DR failover
CSCwc02128	Unable to push device template with security policy with firewall destination port list attached
CSCwc80264	Optional fields is greyed out in Cisco SD-WAN Manager Template Attach page
CSCvz71920	The MT Cisco SD-WAN Manager 20.6 : VPN Dashboard shows nothing
CSCwc15033	The template push fails with 'Failed to update configuration' error on 20.6.3
CSCwc75127	Cisco SD-WAN Manager, Cisco IOS XE SD-WAN device BGP summary counts are incorrect

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.1.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.1.2

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

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.4.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.4.1

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

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5.2

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

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.3.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.3.2

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

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5.1



Note Cisco SD-WAN Controllers Release 20.6.5 is impacted by the defects CSCwb89273 and CSCwd94839 and impacts the performance of Cisco SD-WAN Manager. We recommend you to upgrade to Cisco SD-WAN Controllers Release 20.6.5.1.

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5.1

Identifier	Headline
CSCwd94839	Cisco SD-WAN Manager GUI becomes unavailable due to authentication errors against configuration-db
CSCwb89273	Cisco SD-WAN Manager UI auth failed after running for few hours

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5



Note Cisco SD-WAN Controllers Release 20.6.5 is impacted by the defects CSCwb89273 and CSCwd94839 and impacts the performance of Cisco SD-WAN Manager. We recommend you to upgrade to Cisco SD-WAN Controllers Release 20.6.5.1.

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5

Identifier	Headline
CSCwc13452	Memory leak in Cisco SD-WAN Controller-OMP
CSCwd78294	Screen goes into loading when logged in as a basic user
CSCwa94087	Cisco SD-WAN Manager truncates "0" when we use BGP AS dot notation.
CSCwd01820	Disaster recovery syslogs are set as information priority instead of correct priority
CSCwd20179	Devices not able to perform upgrade when data collection is turned off as site-id is not known.
CSCwc04446	Default route is not installed in the routing table of VPN 0 if the VNIC is changed in OpenStack
CSCwc50308	Frequent GC causing Server Unavailable returing 503, GUI unaccessible intermittently
CSCwd73714	Cisco SD-WAN Manager : DSPFarm template error while configuring "CUCM Media Resource Name"
CSCvx00337	Cisco SD-WAN Manager - Wildfly allocation reduced after upgrade
CSCwc75057	Cisco SD-WAN Manager configuration commit hit Aborted: application communication failure error
CSCvz62264	GCP: Cloud Router uses older version of GCP apis
CSCwc73492	20.10, vBond Hostname "NULL"
CSCwc95935	DCA.py to remove the check for vanalytics to push telemetry data
CSCwa83271	Site List in Cloud OnRamp for SaaS application is not listed
CSCwc14154	[20.6.x] DPI Local TLOC information missing in Cisco SD-WAN Manager Aggregated Data and after enabling ODT
CSCwb19715	BFD and Control flap for entire overlay after pushing WAN Edge list
CSCwc81937	Cisco SD-WAN Manager has extra Netconf Sessions when making API calls
CSCwa68925	20.3.4 -- 2 minutes delay in Webhook event.
CSCwa76773	MT-tenant deletion causes VmonitorAgent log to get stuck and DCA doesn't send information to DCS
CSCwc87356	Cisco SD-WAN Manager "Renew Device CSR" task cannot be opened under completed tasks
CSCwb39591	On Cisco SD-WAN Manager, crash logs are incomplete for containers, occupied more space under /var/crash
CSCwc75127	Cisco SD-WAN Manager cEdge BGP Summary Counts Are Incorrect

Identifier	Headline
CSCwb87891	With 10K Scale post BFD Flap observing socket leak and high memory utilization
CSCwd23369	Standby Cluster configuration is lost during data replication
CSCwb91325	Back button on config preview takes back to device template page
CSCwc80099	After configdb credentials change, app-server is not coming up due to use of hyphen in credentials
CSCwd28593	Control connection flap of assigned Cisco SD-WAN Controller after shutting down other assigned Cisco SD-WAN Controller
CSCwc95869	Memory leak observed when adding a new node to a cluster

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.5

Identifier	Headline
CSCwd96078	Duplicate custom app causing traffic to drop.
CSCwd82147	Not able to create resource group in Cisco SD-WAN Manager 20.6.3
CSCwd94839	Cisco SD-WAN Manager GUI becomes unavailable due to authentication errors against configuration-db
CSCwc85839	Cisco SD-WAN Manager not reporting licenses to CSSM portal
CSCwd96644	Not able to edit the PIM interface for cEdge feature template.
CSCwd32428	SSH from Cisco SD-WAN Manager GUI failing on MT cluster with error "Internal Server Error"
CSCwd31522	20.10 :Edit of single VPC fails to do mapping as required
CSCwd54278	The aaamgr process restarts unexpectedly
CSCwd93750	20.6.3 "BFD Site Down" alarm is not generated on the Cisco SD-WAN Manager.
CSCwd95883	Neo4j credentials on leader node failing after a few hours of being fixed.
CSCwd93156	Block_Cipher.cpp:do_evp_final: Bad ciphertext padding provided
CSCwd97172	Some Cisco SD-WAN Manager logfiles within the admin-tech are very big in size even when compressed
CSCwd94301	MTT correlation engine not generating OMP Alarms from OMP Event received from Cisco SD-WAN Controller
CSCwd60889	CPU average values reported to Cisco SD-WAN Manager are incorrect
CSCwd90586	Cisco SD-WAN Manager scrollbar is executing several API calls that slow down the performance

Identifier	Headline
CSCwd97331	Template push preview inaccurate while shutting down VDSL interface
CSCvz88483	Template Push Failure because of error: Failed to publish the task on message bus
CSCwd85558	The app-server java process is not initiating in 6 node 20.6 cluster
CSCwe14017	Cisco SD-WAN Release 20.6.5: Cisco SD-WAN validator and Cisco SD-WAN Controller upgrade fail via Cisco SD-WAN Manager UI

Bugs for Cisco Catalyst SD-WAN Control Components 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 Catalyst SD-WAN Control Components Release 20.6.4

Identifier	Headline
CSCwa60525	Device template fails due to community string error after upgrade to 20.6
CSCwa85537	Cisco SD-WAN Manager UI stuck forever with {{msg1}} showed on UI while attaching cEdge to device template failed
CSCwc41119	Duplicate Role descriptors found in IDP metadata
CSCvz06108	Enhancement: Cisco VPN Interface IPsec template does not DH group 2 as option
CSCwb68441	VPN drop menu shows empty in NWPI when we iniiate trace for first time
CSCwb35787	20.4 TACACS: old password working after password change on TACACS server
CSCwb37899	CoR Multicloud for GCP Site-to-Cloud CGW Deployment fails with Code 400 in S2S non supported region
CSCvx00337	Cisco SD-WAN Manager - Wildfly allocation reduced after upgrade
CSCwc00863	OMPD crash on policy update
CSCvz35603	VRRP optional fields Server error
CSCwb38187	Cisco SD-WAN Manager - 20.6.2.1 template push failed due to optional field - Invalid value for prefix
CSCwc10636	Replication does not start after system triggered manual switchover
CSCwc10437	20.6.3 to 20.6.4 Cisco SD-WAN Manager upgrade task got stuck in schedule state for Cisco SD-WAN Manager1
CSCwc15033	Template push fails with 'Failed to update configuration' error on 20.6.3
CSCwc15687	New image activation fails with DR paused and a warning message requesting to pause DR

Identifier	Headline
CSCvz87812	Provide "Migrate Device" option in Cisco SD-WAN Manager UI before the device has been onboarded to Cisco SD-WAN Manager
CSCwb20070	20.8 : Disaster Recovery workflow fails during switchover
CSCwb38813	Secondary Cisco SD-WAN Manager continuously generates 'Data Center Down' alarms
CSCwa87469	Enabled usage but prepaid consumption
CSCwc08514	Cisco SD-WAN Manager GUI and CLI has different syntax for usergroup
CSCvz37973	SRST Feature Template "CUCM Media Resource Group" does not accept variable for field
CSCvy01378	Device Specific field is not usable
CSCvz48258	Enabling an application once gateway is attached goes through, but shows app as disabled on Cisco SD-WAN Manager
CSCvz63280	Cisco vEdge Does Not Respond Properly to vSmart Policy Prefix-list Changes (CLI Policy)
CSCwa25355	20.7: Unreachable node still shows up in device list
CSCwa40924	Cisco SD-WAN Manager UI failed to update password
CSCwc22047	IOS XE Devices not able to download policies from vSmart
CSCvz95054	System IP persists after invalidating the edge devices from the Cisco SD-WAN Manager which it is not connected .
CSCwa54969	Cisco SD-WAN Manager iptables-dropped Log stopped after upgrading 20.6.1
CSCvz66256	Filtering the data based on local tloc is returning no data in Cisco SD-WAN Manager GUI for DPI stats
CSCwa87012	Route policy to match multiple community string, Cisco SD-WAN Manager does not generate match community command
CSCwc02128	Unable to push device template with security policy with firewall destination port list attached

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.4

Identifier	Headline
CSCwc04446	Default route is not installed in the routing table of VPN 0 if the VNIC is changed in OpenStack
CSCwc47497	Cisco SD-WAN Manager does not send API calls to cisco.com to a configured HTTP proxy server
CSCwb65034	Search for tunnel is not working

Identifier	Headline
CSCwc27827	Tunnel services cannot be changed of Cellular Gateways from Cisco SD-WAN Manager
CSCwc59865	Cisco SD-WAN Manager statistics-db heap-dump and thread-print commands are not supported
CSCwc05127	Breakdown of U-Plane communication after updating vSmart's CiscoPKI certificate
CSCwc37072	Template failed issue
CSCwc60513	Disk utilization increases on ceph although disk utilization on Cisco SD-WAN Manager doesn't increase
CSCwc62130	Cisco SD-WAN Manager Running 20.6.3 has no option for match VPN on device access control list
CSCwb76421	DPI stats processing is limited to 1 to 1.3 TB per day
CSCwc75057	Cisco SD-WAN Manager configuration commit hit Aborted: application communication failure error

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.3.1

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 Catalyst SD-WAN Control Components Release 20.6.3.1

Bug ID	Description
CSCwc15033	Template push fails with 'Failed to update configuration' error on 20.6.3

Bugs for Cisco Catalyst SD-WAN Control Components 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 Catalyst SD-WAN Control Components Release 20.6.3

Identifier	Headline
CSCwb43423	Cisco IOS XE Catalyst SD-WAN device: IOS XE image installation fails
CSCwb16723	Traceroute not working on Cisco IOS XE Catalyst SD-WAN device with NAT
CSCwb51595	Missing IOS config (voice translation rule) on upgrade from 17.3 to 17.6
CSCwa67886	UDP based DNS resolution doesn't work with IS-IS EMCP on IOX-XE
CSCwb33968	Cisco SD-WAN Manager failed to display active flows when flow count is high on the device.

Identifier	Headline
CSCvz84588	Destination prefix packets getting dropped because forwarding plane is not programming the next hop.
CSCwb59736	CSR BFD tunnel are zero with SDWAN version 17.03.03.0.7
CSCwb44275	Simulated flows with PPPoE with NAT DIA result in crash consistently over Utah platform
CSCwa57873	Incorrect reload reason - Last reload reason: LocalSoft for Netconf Initiated request
CSCwb18223	SNMP v2 community name encryption problem
CSCwb18315	Umbrella DNS security policy doesn't work with Cloud onRamp with SIG tunnels
CSCwa49721	SDWan HUB with firewall configured incorrectly dropping return packets when routing between VRFs
CSCwb13820	C8Kv crashed at high scale with IPSEC and heavy features configured
CSCwb39098	Router crashed after new IPv6 address assigned when router use specific configuration

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.3

Bug ID	Description
CSCwb38813	Secondary Cisco SD-WAN Manager continuously generates 'Data Center Down' alarms
CSCwb97344	Cisco SD-WAN Manager cluster upgrade from 20.3.4.1 to 20.6.3 : configuration-db upgrade failed
CSCwc02128	Unable to push device template with security policy with firewall destination port list attached
CSCvy72764	Services still communicate via old OOB IP after changing the vpn 0 OOB interface IP
CSCwb20070	Disaster Recovery workflow fails during switchover
CSCwa76773	MT-tenant deletion causes VmonitorAgent log to get stuck and DCA doesn't send information to DCS
CSCwa87469	Enabled usage but prepaid consumption
CSCvz60689	Cisco SD-WAN Manager with IPv6 interface with local user fails until we login with ipv4 once
CSCwb38187	Cisco SD-WAN Manager - 20.6.2.1 template push failed due to optional field - Invalid value for prefix
CSCwa90832	App-Server continuously restarting after the restore of config-db during Active-Backup Restore

Bug ID	Description
CSCwa21248	Boot up time to bring up the containers takes considerable amount of time in 20.6 compared to 20.5
CSCwb61136	Cisco IOS XE SD-WAN Device: "platform console serial" command is removed unexpectedly after Cisco SD-WAN Manager push template
CSCwc15033	Template push fails with 'Failed to update configuration' error on 20.6.3

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.2.2

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 Catalyst SD-WAN Control Components Release 20.6.2.2

Bug ID	Description
CSCwa54712	Evaluation of Cisco Catalyst SD-WAN for Log4j 2.x DoS vulnerability fixed in 2.17

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.2.1

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 Catalyst SD-WAN Control Components Release 20.6.2.1

Bug ID	Description
CSCwa47745	Evaluation of Cisco SD-WAN Manager for Log4j RCE (Log4Shell) vulnerability

Bugs for Cisco Catalyst SD-WAN Control Components 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 Catalyst SD-WAN Control Components Release 20.6.2

Bug ID	Description
CSCvx00337	Cisco SD-WAN Manager - Wildfly allocation reduced after upgrade
CSCvy33818	On MTT Cisco SD-WAN Manager system IP persists after invalidating and deleting the edge devices.
CSCvy44723	control connection to the edege device doesnt come up with v6 and reverse proxy
CSCvy89137	"show support omp peer" not available - replacement for "show internal omp peer"
CSCvy89347	Advertisement-interval delays withdrawal even if there was no previous update message and stable rib

Bug ID	Description
CSCvy96800	Feature template for OPSF default-origination metric doesn't save changed variable names
CSCvy97321	omp route propagation delays due to constant marker resets on TLOC flap
CSCvy97925	vEdge Local configuration not showing up under GUI
CSCvy99978	2.5 MT Cisco SD-WAN Manager generate wrong configuration for app-list <ftp&ftp-data>
CSCvz16944	Multicloud Monitoring Dashboard does not show any data when login as provider and switch to tenant
CSCvz18399	20.5.1 Cisco SD-WAN Manager aggregate optional field is not considered as optional
CSCvz25427	tenant login privilege is denied if local radius tacacs auth is configured
CSCvz26464	Renew CSR MTT- Cluster : Alarms for WANedge software device cert expiration is not generating tenant
CSCvz26738	cfgmgr crashed while trying to delete / create tenant in Multi Tenant lead to vdaemon crash
CSCvz30541	In 20.6, Device with 17.5.1, AppQoE TCP opt graphs are not displayed.
CSCvz31909	Disaster Recovery is failing to export the config-db in standby DR
CSCvz36007	cloudagent-v2 gets stuck at host discovery
CSCvz36335	UI didn't comeup when 2nd node was a compute node
CSCvz39917	Failed to find VPN mapping for cloudType:{} after upgrade from 20.4.2 to 20.6.1
CSCvz43823	Cisco SD-WAN Manager is not able to discover VPCs for Multi-cloud when >14 AWS accounts provisioned
CSCvz48262	Unable to enable PnP Connect
CSCvz49235	Software activation via UI failing even when DR replication is paused
CSCvz49299	Cisco SD-WAN Manager services do not start on upgrade from 20.3 to 20.6 due to upgrade-context.json incorrect
CSCvz51928	Interface Endpoints isn't updated when tunnel refresh button is used
CSCvz55034	Cisco SD-WAN Manager 20.6.1 Dashboard does not show custom application server logo
CSCvz55982	Incorrect error message during NWPI Trace configuration
CSCvz65205	Resource group not working on Cisco SD-WAN Manager 20.6.1
CSCvz67290	Not able to copy or add new Voice Policy in Cisco SD-WAN Manager 20.6.1

Bug ID	Description
CSCvz69856	Cisco SD-WAN Manager - After upgrade to 20.4.2 or 20.6.1 feature template field is not optional anymore
CSCvz73489	API to fetch control summary is not working in 20.5 or later release
CSCvz75378	"The status code is missing in the response from server" when filtering on devices groupId
CSCvz07202	Tenant creation is failing on 20.3.3 MT cluster vmanage
CSCvz62234	Cisco Catalyst SD-WAN Manager Unauthorized Configuration Rollback Vulnerability

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.2

Bug ID	Description
CSCvy01378	Device Specific field is not usable
CSCvy31077	Cisco SD-WAN validator upgrade from 20.4.1 to 20.5.1 may fail due to upgrade-confirm not received
CSCvy39355	CSR generation fails if given OU differs from org-name on the Cisco SD-WAN Manager
CSCvy72764	services still communicate via old OOB IP after changing the vpn 0 OOB interface IP
CSCvy87142	valid-vedges list in Cisco SD-WAN Manager and Cisco SD-WAN validator are not consistent after send to controller
CSCvz02667	Cisco SD-WAN Manager ODT : Monitoring Stats collection takes > 3 hours when selected for 1 day duration.
CSCvz03954	Update Cisco SD-WAN Manager clustering support to CloudDock
CSCvz05132	CoR SaaS "vQoE Score History" not getting displayed for vEdge on Cisco SD-WAN Manager
CSCvz28684	Huge Data replication observed during DR process of 3 node cluster running 20.3.4
CSCvz30153	ES(ex. Alarm/Event/Audit) replication import fail
CSCvz32341	custom application list not replicated in Disaster Recovery for a Single Node Cisco SD-WAN Manager Cluster
CSCvz34413	replication will start from time 0 if replication leader entry not present replicationstatus table
CSCvz40247	Security policies applied to incorrect interface in cluster mode, iptables
CSCvz46043	Device inventory sections shows incorrect count.
CSCvz50700	Error occurred while generating report

Bug ID	Description
CSCvz53305	Cisco SD-WAN Manager: Local device access policy with SNMP is not getting pushed correctly.
CSCvz60689	Cisco SD-WAN Manager with IPv6 interface with local user fails until we login with ipv4 once
CSCvz67260	Generate Bootstrap Configuration for c8300 is not working, Cisco SD-WAN Manager 20.6.1
CSCvz68624	Login to Viptela OS fails if plain-text password was set in cloud-init write_files
CSCvz75471	New sequence in RPL with set as-path has both prepend and exclude as required fields
CSCvz87812	Provide "Migrate Device" option in Cisco SD-WAN Manager UI before the device has been onboarded to Cisco SD-WAN Manager
CSCvz89536	[MSDC] 20.6.2: API delay of 90+ seconds in displaying Real Time Tunnel statistics
CSCvz95054	System IP persists after invalidating the edge devices from the Cisco SD-WAN Manager which it is not connected.
CSCvz89254	Cisco SD-WAN Manager config roll back failed after Cisco SD-WAN Manager template is attached to the Cisco IOS XE SD-WAN device.
CSCwa32801	config-db memory climbing up on MT scale setup
CSCwa17310	template attach fails after upgrading to 20.6.2 from 20.4.2
CSCvz94799	MTT : OptIn status is not updated to the Cisco IOS XE SD-WAN devices in a tenant
CSCwa25256	Installing new enterprise wan edge cert does not remove old cert causing device to use old cert
CSCvz80036	vEdge_Nitro: google-accounts getting classified as google-services in DPI Application
CSCwa23351	NWPI fail to merge domain/IP for dual Cisco IOS XE SD-WAN device site
CSCwa21248	boot up time to bring up the containers takes considerable amount of time in 20.6 compared to 20.5
CSCwa56750	MTT, site/node level alarm are missing when manually shutdown / re-start edge device

Bugs for Cisco Catalyst SD-WAN Control Components 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 Catalyst SD-WAN Control Components Release 20.6.1

Bug ID	Description
CSCvm52858	Incorrect referencing to SHA on Data plane (GCM)

Bug ID	Description
CSCvs66726	Cluster deactivate is not supported when cluster is stuck in init state
CSCvt63483	Cisco SD-WAN Manager: neo4j transient exception - database not upto the required version
CSCvv13313	Select control connection TAB for any vsmarts, it will never show vbond connections
CSCvv31205	Network Design - Unable to add Services due to Cisco IOS XE SD-WAN device SNMP global parameters is set
CSCvv50436	Cisco SD-WAN Manager WebServer uses a hard coded self-signed certificate
CSCvv99743	High failure API rate when device is not directly connected to the API query receiver
CSCvw31595	SG attach fails with Placement Failed Error - VM BW not met even though there are no SC's attached
CSCvw36009	Cisco vBond/ Cisco vSmart Upgrade Failed and Rollback due to Upgrade confirm not received.
CSCvw45408	Azure Node:Device Upgrade task stuck when 1 Cisco SD-WAN Manager node goes for a reboot
CSCvw48486	Cisco SD-WAN Manager email notifications not working
CSCvw54692	Cisco IOS XE SD-WAN device Unable to configure ospf simple password authentication
CSCvw55764	VNF Install fail - VNF packages are not sync'd/copied in new added Cisco SD-WAN Manager node in Cisco SD-WAN Manager cluster
CSCvw56471	Upgrade 20.3->20.4, ND Profile->LAN page does not show global vlan, spanning-tree and native-vlan
CSCvw57727	Backward Compatibility:20.4 LAN global vlan config does not automatically translate for NFVIS 4.2
CSCvw69475	Cisco SD-WAN Manager MTT Cluster - Cisco SD-WAN Manager Active to Backup restore does not work
CSCvw92020	Checkbox is not usable under Update Device Template tab
CSCvx00337	Cisco SD-WAN Manager - Wildfly allocation reduced after upgrade
CSCvx02370	Add device check for alarm process
CSCvx11296	Cisco IOS XE SD-WAN device reporting normal even though it is over warning threshold
CSCvx14674	ENH: make media-type rj45 available in the interface template
CSCvx18282	ND Profile -> LAN preview does not show global VLAN, spanning-tree and/or trunk native VLAN info

Bug ID	Description
CSCvx30650	Generic SIG template is not getting added to device Template
CSCvx34991	Cisco SD-WAN Manager - TACACS requests are sourced from old interface IP after IP changed
CSCvx43560	template push fails when entire device config is passed as a input variable
CSCvx44834	ASR1K - ACE entry added after object-group is missing in hardware causing packets drops
CSCvx57103	Cisco SD-WAN Manager: Template push may fail after upgrading to 20.4
CSCvx62993	Cisco SD-WAN Manager: motd api will retrieve line break by removing the slash character and keeping "n"
CSCvx68299	Template Update: "Error occurred while generating inputs for device templates. Please try again... "
CSCvx70706	Adding a new SC to an attached SG when no resources available saves SC although SC not provisioned
CSCvx72147	Unable to generate Admin tech via GUI
CSCvx76036	View of dashboard Cisco SD-WAN Manager for (OMP sessions) in Multi-Tenant
CSCvx79831	Call Feature Template: Number Pattern does not accept characters '[ ]' , '$' and '^'
CSCvx80917	Cisco SD-WAN Manager monitor-realtime ospf neighbor/interface incorrect
CSCvx82823	Destination device drop-down doesn't show devices after speed test run
CSCvx89235	MTT : SD-AVC REST APIs calls task stuck in scheduled state after creating / editing custom appli
CSCvx89314	Data collection status stuck in Queued state after performing VNF start/stop/reboot
CSCvx93652	Push vEdge list fails to vSmart with application error.
CSCvx94934	df -kh output is misleading and Cisco SD-WAN Manager platform until we reload the VM
CSCvx95333	Use new format of cloud-init for bootstrap of vEdge Cloud >=20.5
CSCvx98106	Cisco SD-WAN Manager user sessions not getting cleaned up, approx 19700 active sessions
CSCvx99730	vBond restart happens after "show orchestrator unclaimed-vedges ?" command
CSCvy00144	Setting logging console to disabled does not work in Cisco SD-WAN Manager global settings feature template
CSCvy00234	API Docs for /device/ip/ipRoutes doesn't filter for VPN correctly
CSCvy01922	Cisco SD-WAN Manager cert issue during a Cluster build due to certifcate issue

Bug ID	Description
CSCvy03296	CLI Template variables appear in reverse alphabetical order.
CSCvy05380	6 node Cisco SD-WAN Manager device list page refreshing in 30 sec with GET API : dataservice/system/device/vedges
CSCvy11479	user from resource-group can manage global resources
CSCvy12594	Cisco SD-WAN Manager REST API response 403 is sent in incorrect Content-type HTML format, should be JSON
CSCvy14263	20.6 Controller Upgrade failed: NetConf: Connection to device failed during install.
CSCvy14627	Activating changes in Security Policy that is attached to the vEdge will fail and lock the database
CSCvy14765	Cisco SD-WAN Manager doesn't apply TCP MSS configuration under SIG tunnel if it's set to default in SIG template
CSCvy15370	Cisco SD-WAN Manager API running too frequently under Rediscover Network resulting in Page Loading too often
CSCvy20437	ciscotacro/rw disablement via CLI template fails
CSCvy22617	206/next-vmanage:LATEST: deploy in esxi: traceback/crash & stuck observed while first login
CSCvy22914	Cisco SD-WAN Manager GUI down 20.3.3 due to Full GC (Allocation Failure)
CSCvy23515	Cisco SD-WAN Manager/20.5.1/Warning: Chassis Number is Mandatory for Cisco Devices// They are installed in the db
CSCvy24936	vBond connections continuously flapping on edge devices.
CSCvy25919	Cloud OnRamp: Available Regions not listing all regions that AWS account has access to
CSCvy26980	Unknown error: Unable to update or delete user credentials for existing AWS/Azure acount
CSCvy27219	Cisco SD-WAN Manager GUI is down after /opt/data fills with heapdump
CSCvy29280	NullPointerException in getMasterTemplateDefinition when retrieving template details
CSCvy32540	DB_upgrade failed because of one NMS service failed to start.
CSCvy33818	On MTT Cisco SD-WAN Manager system IP persists after invalidating and deleting the edge devices.
CSCvy34295	CLI request nms configuration-db update-admin-user does not change user password on rest of Cisco SD-WAN Manager
CSCvy34380	Cisco SD-WAN Manager 20.5.1 Security Policy Can't have match protocl Name and Destination Port number

Bug ID	Description
CSCvy35142	"App Route Statistics" won't display statistics for Cisco IOS XE SD-WAN devices on 20.4.x
CSCvy43320	Request support to have "ciscotac" internal commands
CSCvy45393	During Cisco SD-WAN Manager cluster creation, the primary Cisco SD-WAN Manager did not send the S/N to load share the CC
CSCvy50083	Devices->Local Configuration , Split Screen while viewing the Local configuration , screen attached
CSCvy60555	Rollback of GCP CGW does not complete if Compute Alpha API is are not enabled or Quota limit hits
CSCvy63368	How to add missing Sudi_chassis in Cisco SD-WAN Manager running 20.5 before upgrade to 20.7
CSCvy66979	[SIG template] Values greater than 255 for idle-time and refresh-time for Zscaler are unconfigurable
CSCvy71956	206/176 : ztp upgrade not triggered and stuck at 'Sync Pending - Software upgrade after ZTP'
CSCvy73412	Templatepush failed for C8300-2N2S-4T2X with error bad-cli-negotiation auto,parser-context
CSCvy75420	Cisco SD-WAN Manager reports 'upgrade request failed in device' error after installing the software via ZTP
CSCvy77151	Unable to add user in SNMP Feature Template
CSCvy79095	configuration db VMANAGE ROOT CA node is not updated
CSCvy82153	Login Success for deleted Cisco SD-WAN Manager local user
CSCvy82285	KVM vbond if-oper-status down after reboot by Cisco SD-WAN Manager APi (support Redhat*)
CSCvy85092	Admin user logged in Cisco SD-WAN Manager with logging auth group
CSCvy88437	AWS VPN based: IPSEC tunnels from CGW C8kvs to TGW down on latest 20.6 build
CSCvy88637	Cisco SD-WAN Manager email notification - supporting special character & (ampersand) in the email address
CSCvy93596	application services goes OOM due to user session node deletion as part of startup in Cisco SD-WAN Manager
CSCvy93992	Enforce Software Version(ZTP) does not work as expected on Multi Tenant setup
CSCvy94112	request nms server-proxy stats does not work
CSCvy97925	vEdge Local configuration not showing up under GUI

Bug ID	Description
CSCvz04803	MTT, Missing OMP down Alarms(tloc, node, site) after device is unreachable
CSCvz16670	OMP node down cannot generate when change system-ip
CSCvz30626	20.6: Cisco SD-WAN Manager Main Dashboard , with Top Application Data => SSL proxy, data is empty
CSCvw59643	Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.6.1

Bug ID	Description
CSCvw81892	[SIT] AWS instance Cisco SD-WAN Manager unable to reach devices after upgrade to 20.5.999 image
CSCvx44834	ASR1K - ACE entry added after object-group is missing in hardware causing packets drops
CSCwc80099	After configdb credentials change, app-server is not coming up due to use of hyphen in credentials
CSCvx46554	Cisco SD-WAN Manager reverting API changes after 5 minutes
CSCvx79376	Cisco SD-WAN Manager UI showing empty group value when editing device values
CSCvy01378	Device Specific field is not usable
CSCvy31077	vBond upgrade from 20.4.1 to 20.5.1 may fail due to upgrade-confirm not received
CSCvy33818	On MTT Cisco SD-WAN Manager system IP persists after invalidating and deleting the edge devices.
CSCvy38478	Cisco SD-WAN Manager ver 19.2.4 crash, becomes unstable/unusable
CSCvy39355	CSR generation fails if given OU differs from org-name on the Cisco SD-WAN Manager
CSCvy44723	control connection to the edege device doesnt come up with v6 and reverse proxy
CSCvy63270	Cisco SD-WAN Manager is not generating/sending "endpoint-tracker" command to interface (Cisco IOS XE SD-WAN device)
CSCvy72764	services still communicate via old OOB IP after changing the vpn 0 OOB interface IP
CSCvy77303	Cisco IOS XE SD-WAN device template throws internal error via feature template to just one device
CSCvy82286	Inconsistent response from Cisco SD-WAN Manager API to generate bootstrap in 20.5.1
CSCvy84892	vSmart doesn't establish control connection with Cisco SD-WAN Manager in 20.5.1 reason:"ERR_SER_NUM_NT_PRESENT"

Bug ID	Description
CSCvy87142	valid-vedges list in Cisco SD-WAN Manager and vbond are not consistent after send to controller
CSCvy89137	"show support omp peer" not available - replacement for "show internal omp peer"
CSCvy96335	During ZTP Cisco SD-WAN Manager pushes template before SW was upgraded up to minimal required
CSCvy99978	2.5 MT Cisco SD-WAN Manager generate wrong configuration for app-list <ftp&ftp-data>
CSCvz02667	Cisco SD-WAN Manager ODT : Monitoring Stats collection takes > 3 hours when selected for 1 day duration.
CSCvz03954	Infra query not send to all CSPs by Cisco SD-WAN Managers in cluster causing CD Cluster to Fail
CSCvz05132	CoR SaaS "vQoE Score History" not getting displayed for vEdge on Cisco SD-WAN Manager
CSCvz05221	Impossible to install UTD software with "Task cannot proceed. Similar task is in progress" error
CSCvz07161	20.6 / 17.6 : Custom Apps do not work with working Cisco SD-WAN Manager going down in cluster
CSCvz14731	Cisco SD-WAN Manager detects Viptela OS on ISR 1100 even if its running IOS XE
CSCvz14915	[MT-MT Migration]Unable to see OMP seesions on tenant dashboard after migration from 20.3 to 20.6
CSCvz16944	Multicloud Monitoring Dashboard does not show any data when login as provider and switch to tenant
CSCvz25190	20.6 EFT Drop2 HTTP(S) Proxy configuration
CSCvz28541	Possible day 0 issue: software upload fails if Cisco SD-WAN Manager session times out during the process
CSCvz28684	Huge Data replication observed during DR process of 3 node cluster running 20.3.4
CSCvz29468	" Signature trust establishment failed for metadata entry " on Cisco SD-WAN Manager Error
CSCvz30124	20.6 MT provider: when template is detached, password for "admin" can be changed but UI throws error
CSCvz30153	ES(ex. Alarm/Event/Audit) replication import fail
CSCvz30626	20.6: Cisco SD-WAN Manager Main Dashboard , with Top Application Data => SSL proxy, data is empty

Bug ID	Description
CSCvz31054	Cisco SD-WAN Manager Tunnel States API is not backward compatible between 20.6 and 20.4.1
CSCvz31290	Cisco SD-WAN Manager is not pushing the tracker to an interface on Cisco IOS XE SD-WAN device under "VPN Interface Ethernet" template
CSCvz31540	Cisco SD-WAN Manager GUI: upstream connect error or disconnect/reset before headers
CSCvz31909	1+1 DR is failing to export the config-db in standby DR
CSCvz32341	custom application list not replicated in Disaster Recovery for a Single Node Cisco SD-WAN Manager Cluster
CSCvz33123	Shared clouddock cluster activation shows FAILED after claiming its successful
CSCvz34413	replication will start from time 0 if replication leader entry not present replicationstatus table
CSCvz36007	cloudagent-v2 gets stuck at host discovery
CSCvz36335	UI didn't comeup when 2nd node was a compute node
CSCvz36420	LiveAction and other token logins are failing for Cisco SD-WAN Manager
CSCvz37973	SRST Feature Template "CUCM Media Resource Group" does not accept variable for field
CSCvz38091	csrf.properties file is not updated in an upgrade from 20.4 to 20.6
CSCvz38128	For ODT driven Graphs, could see data for old duration timestamps, in-stead of requested time-stamp
CSCvz40247	Security policies applied to incorrect interface in cluster mode, iptables
CSCvz30541	In 20.6, Device with 17.5.1, AppQoE TCP opt graphs are not displayed.
CSCvz39917	Failed to find VPN mapping for cloudType:{} after upgrade from 20.4.2 to 20.6.1
CSCvz37616	Template attach fails during localized policy execution
CSCvz25427	20.6 LATEST: Tenantadmin seeing basic privileges- javax.ws.rs.ForbiddenException: HTTP 403 Forbidden
CSCvz40568	Server error: illegal reference ncs devices

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.

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

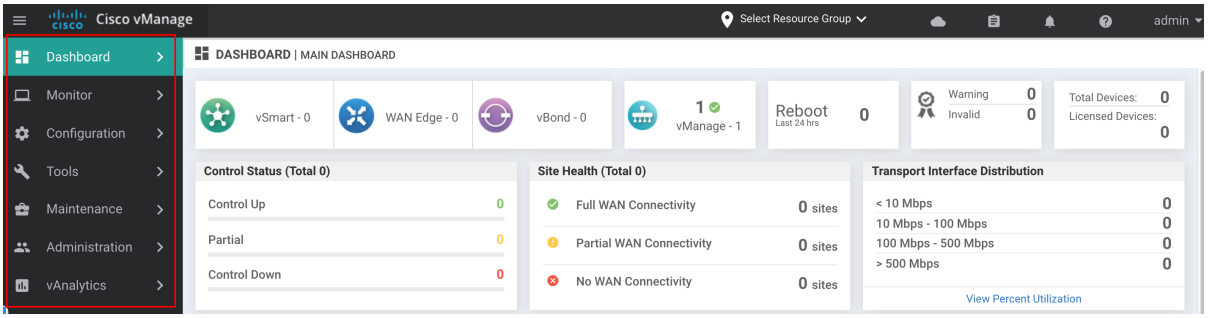


Figure 2: Navigation Menu (Collapsed) in Cisco vManage Release 20.6.1 and Later

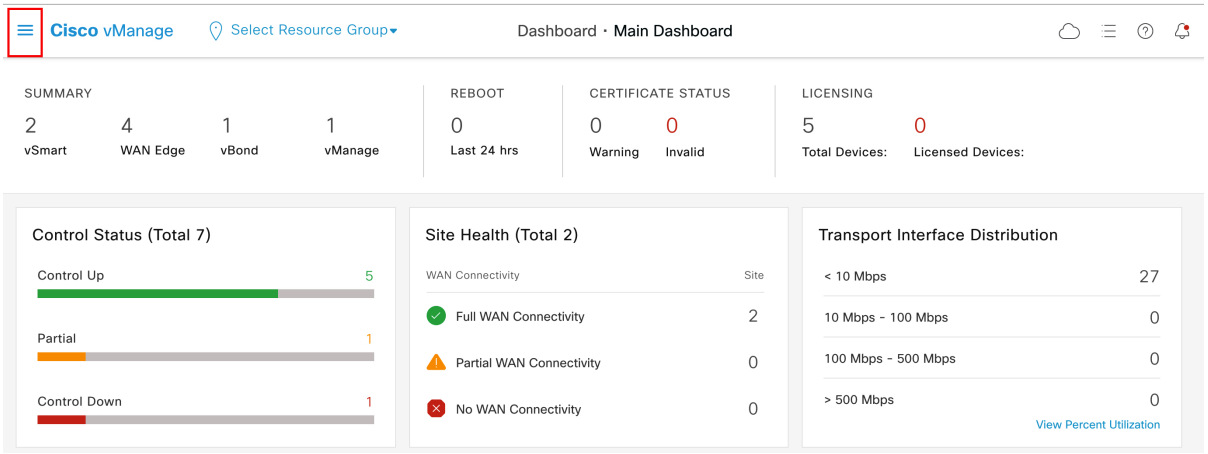
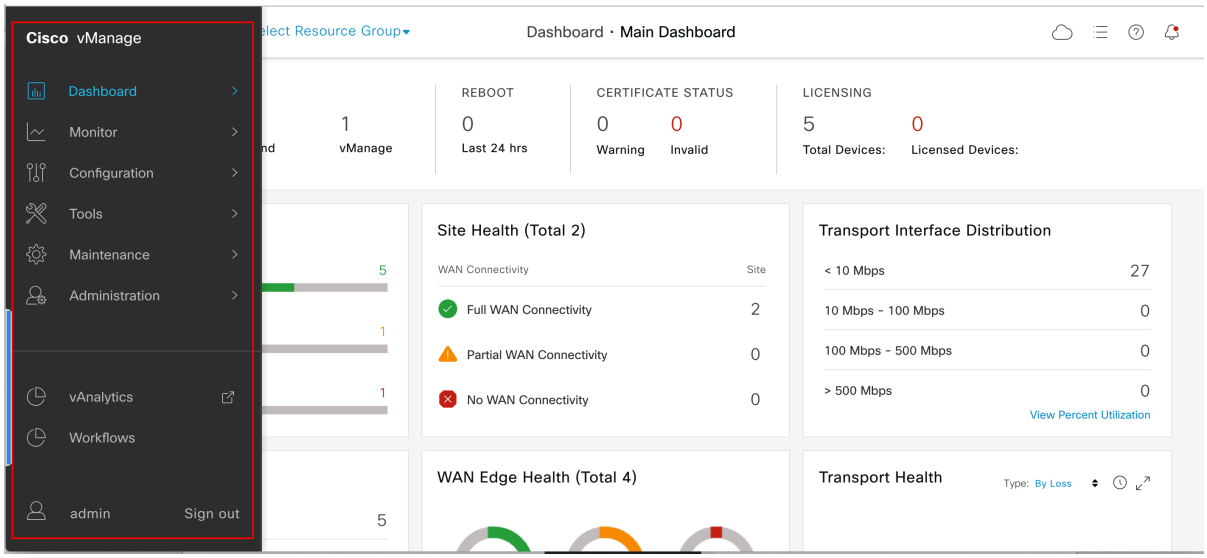


Figure 3: Navigation Menu (Expanded) in Cisco vManage Release 20.6.1 and Later



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

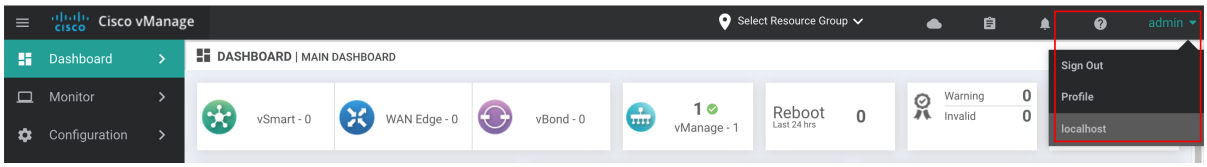
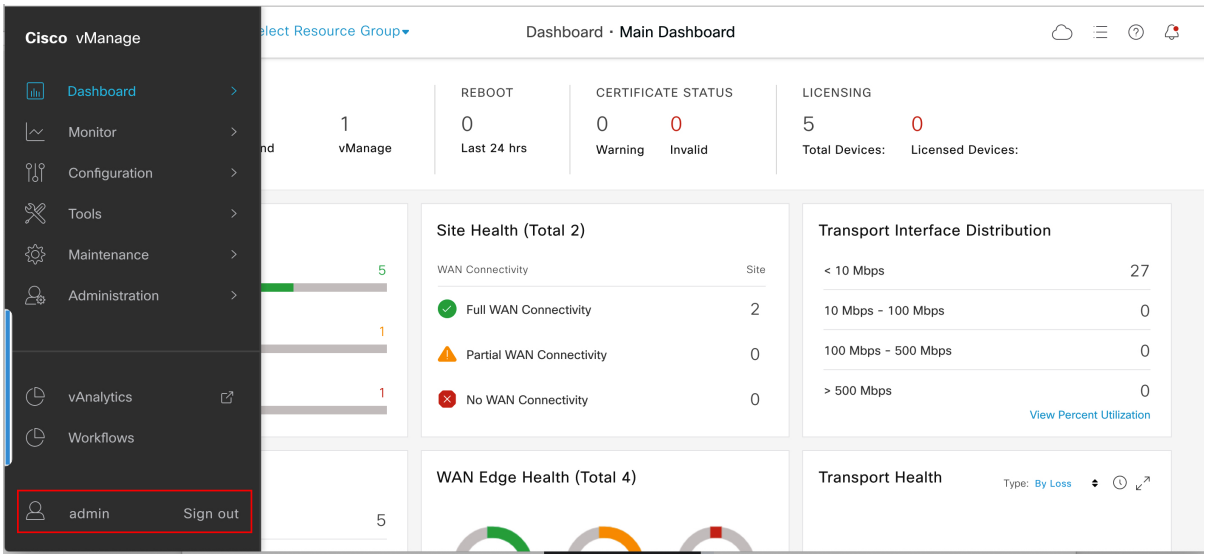


Figure 5: User Profile and Sign Out Options in Cisco vManage Release 20.6.1 and Later



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

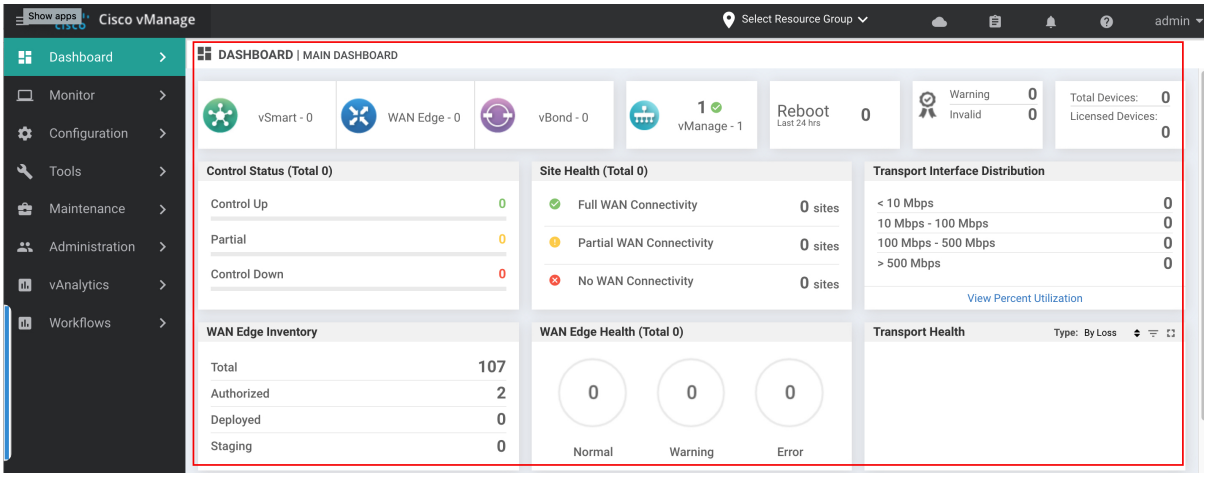
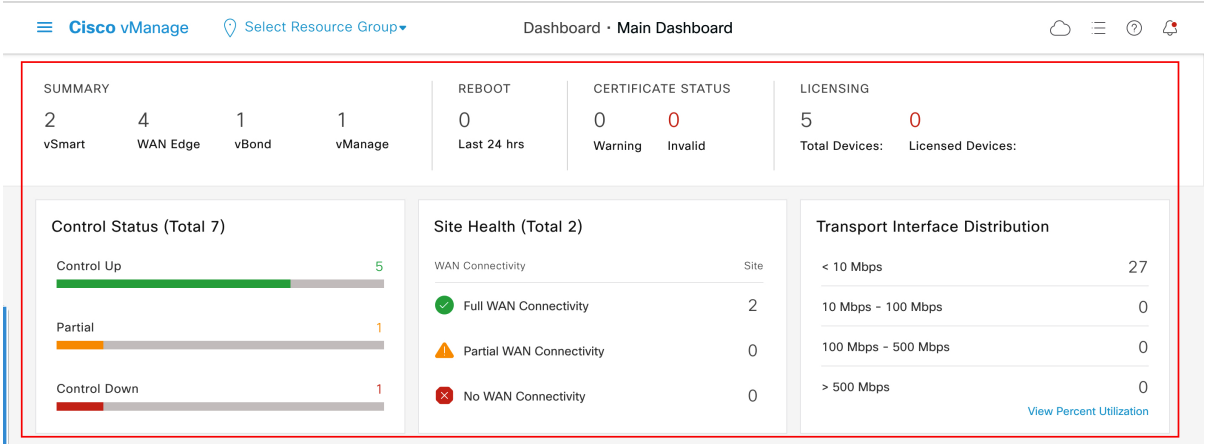


Figure 7: Main Dashboard in Cisco vManage Release 20.6.1 and Later



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

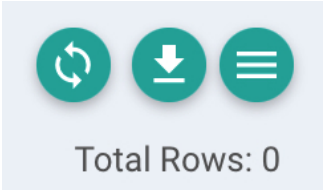


  Figure 9: Example of Icons in Cisco vManage Release 20.6.1 and Later



- 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

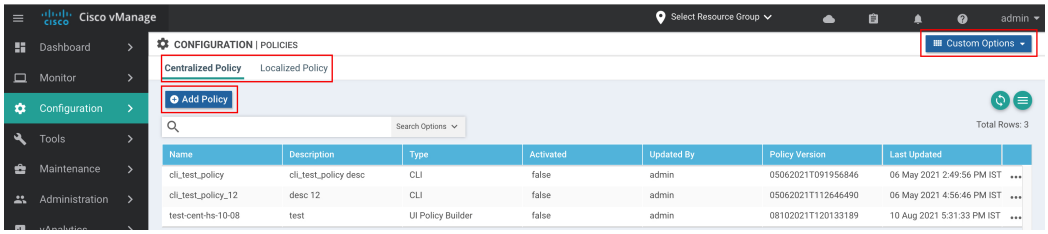
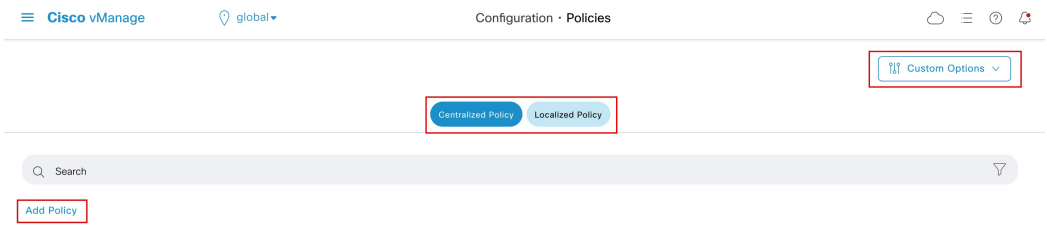


Figure 11: Example of GUI Elements in Cisco vManage Release 20.6.1 and Later



- 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

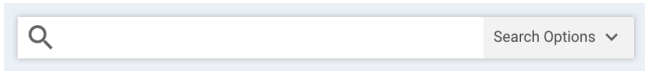
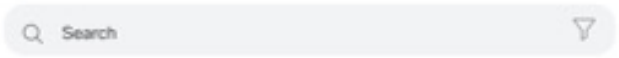


Figure 13: Example of Search Bar in Cisco vManage Release 20.6.1 and Later



Related Documentation

- Release Notes for Previous Releases
- Software Installation and Upgrade for vEdge Routers
- Field Notices
- Recommended Releases
- Security Advisories
- Cisco Bulletins
- Cisco Recommended Catalyst SD-WAN Software Versions for Controllers and WAN Edge Routers

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)

© 2023–2024 Cisco Systems, Inc. All rights reserved.