Release Notes for Cisco Catalyst SD-WAN Control Components Release 20.16.x

First Published: 2024-12-23

Last Modified: 2026-04-29

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 SD-WAN Control Components, Cisco Catalyst SD-WAN Manager Release 20.16.1

These release notes accompany the Cisco Catalyst SD-WAN Control Components, Release 20.16.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 Catalyst SD-WAN.

Related Releases

For release information about Cisco IOS XE Catalyst SD-WAN devices, refer to Release Notes for Cisco IOS XE Catalyst SD-WAN device, Cisco IOS XE Release 17.16.x.

What's New for Cisco Catalyst SD-WAN Manager Release 20.16.1

Cisco is constantly enhancing the Cisco Catalyst SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides.

Table 1: Cisco Catalyst SD-WAN Manager Release 20.16.1

Feature	Description
Cisco Catalyst SD-WAN Monitor and Maintain	
Improved Monitoring of Cellular-Enabled Devices	This feature enhances the cellular monitoring dashlets in Cisco SD-WAN Manager to provide additional insights for building and maintaining a competitive cellular WAN solution. The following dashlets have been enhanced: • Cellular Device Count • Cellular Health • Cellular Data Usage
Manage Log Size	This feature lets you temporarily increase the log size for troubleshooting purposes.
Cisco Catalyst SD-WAN Systems and Interfaces	
Statistics Database Upgrade	Cisco SD-WAN Manager utilizes an upgraded database to improve performance.

Table 2: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started	
Expired Certificate Indication and Quarantine	Cisco SD-WAN Manager indicates when devices or Cisco Catalyst SD-WAN Control Components have expired certificates. Additionally, you can quarantine all edge devices that have expired certificates. Quarantine places devices into the staging status. Quarantined devices keep their control connections to Cisco Catalyst SD-WAN Control Components, but do not handle data plane traffic.
Cisco Catalyst SD-WAN Systems and Interfaces	
Cellular Module Support for Cisco Catalyst Rugged Series Routers	Support for cellular modules on Cisco Cisco Catalyst IR1101, IR1800 and IR18340 Rugged Series Routers.
Cellular Network Slicing	This feature allows multiple networks to exist on the same physical network to optimize the network for different traffic types.
Cisco ThousandEyes Support for Additional Devices in Cisco ISR 1100 Series Routers	Extended Support of Cisco ThousandEyes Enterprise agent to additional devices on Cisco ISR 1100 Series Routers.
Simplified Workflow for Onboarding Cisco ThousandEyes Agent and Configuring Tests	This feature provides a simplified workflow to easily onboard Cisco ThousandEyes agent and configure tests using Cisco SD-WAN Manager.
Configure RADIUS and TACACS Servers to Receive Authentication Requests Over Management VPN 512	This feature provides increased security by allowing you to configure tenants to send and receive AAA traffic over WAN transport VPN 0 or management VPN 512. For more information, see Configure Remote AAA.
Support for Multitenancy Providers to View Tenant's Alarms and Events	This feature allows providers to view tenant alarms and events. Multitenancy providers can enable or disable this feature for each tenant.

Feature	Description
Support for Remote AAA and Webhook Notifications Over Management VPN 512	This feature provides increased security by allowing you to configure tenants to receive AAA traffic and webhook notifications over management VPN 512.
Support for Tenant to Access to Controller-Specific Information	This feature enables tenants to access their controller-specific restricted information, which enhances visibility and simplifies management and troubleshooting within the Cisco Catalyst SD-WAN network. This improved visibility aids in addressing issues related to OMP, routing, control connections, and more.
Upstream and Downstream Bandwidth Reference Values	Use the upstream and downstream bandwidth reference values to govern how Cisco SD-WAN Manager displays interface utilization percentages in charts. The values also act as configurable thresholds that trigger interface-bw events when a network interface's utilization exceeds a defined point.
Cisco Catalyst SD-WAN Security	
Disabled Weak SSH Encryption Algorithms	For better security, certain weak SSH encryption algorithms are disabled by default on port 22 and port 830 for devices in the Cisco Catalyst SD-WAN overlay.
MACsec Support for Cisco Catalyst IR1101 and IR1800 Rugged Series Routers	This feature adds MACsec support for Cisco Catalyst IR1101 and IR1800 Rugged Series routers.
Unified Logging Records Include Logs of Inspect, Pass or Drop Actions	This feature allows generating log data of inspect, pass, or drop actions about security connection events when Unified Logging is enabled.
Cisco Catalyst SD-WAN Cloud OnRamp	
Cloud OnRamp for Multicloud	This feature provides a single common dashboard in Cisco SD-WAN Manager that displays unified information of accounts, gateways, and connections for both cloud and interconnect providers. This feature enhances the user experience by helping you identify resources and monitor each provider's utilization.
Cisco Catalyst SD-WAN Monitor and Maintain	
Data Plane CPU and Memory Utilization	With this feature you can monitor data plane CPU and memory utilization on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager.
Energy Management	This feature introduces a new dashboard that displays the Cisco SD-WAN Manager power utilization, energy usage, device capability, and consumption data.

Feature	Description
Multiple Remote Devices and Circuits to View Tunnel Health	With this feature, add multiple remote devices and circuits to view the tunnel health data in the line chart. You can add a maximum of five devices at a time and the tunnel health data is displayed for each path.
Cisco Catalyst SD-WAN NAT	
Mapping of Address and Port Using Encapsulation (MAP-E) with Transport Locator (TLOC)	This feature extends the support for IP over Ethernet (IPoE) MAP-E to include TLOC interfaces. The integration of MAP-E with TLOC allows the device to handle IPv4 traffic efficiently over an IPv6 network.
Support for Site-Local Failover for NAT DIA	Support for NAT DIA traffic failover in sites with more than one edge device. The support for same-site NAT DIA local failover works with NAT44 and NAT66 by tunneling the traffic from one edge device to another edge device that has NAT DIA access within a site.
Cisco Catalyst SD-WAN Policy Groups	
Application Compliance	When you update the reference Protocol Pack, Cisco SD-WAN Manager checks whether any protocols in the Protocol Pack introduce name conflicts with currently defined custom applications. If so, Cisco SD-WAN Manager does not complete the update of the reference Protocol Pack.
Cloud-Sourced Applications	Cloud-sourced applications, derived from the Cisco SD-AVC component, complement applications from other sources, such as Protocol Packs and custom applications. You can use cloud-sourced applications in security and centralized policies, and in Cloud OnRamp for SaaS.
Configure Source Interface for Security Logging	This feature enables configuring source interfaces for High-Speed Logging (HSL) and SysLog for security logging in Cisco SD-WAN Manager.
Enhancements to Security Policy Using Policy Groups	The following enhancements are introduced with this release: • **Embedded Security** is called **NGFW** in Cisco SD-WAN Manager. • Create copies of security policy and sub-policy. • View all configured rules for specific policies in the **NGFW** policy dashboard. • For each rule, **Clone rule**, **Add rule on top**, and **Add rule below** options are added.
Server Label For High Speed Logging Source Interface and External Syslog Source Interface	This feature allows users to configure the High-Speed Logging Source Interface and SysLog Source Interface for security logging based on the security policy level for SD-WAN.
Cisco Catalyst SD-WAN Network-Wide Path Insight User	

Feature	Description
Synthetic Traffic Packet Capture Replay	With this feature, you can simulate traffic of a trace by replaying a PCAP file.
Cisco Managed Cellular Activation	
Managed Cellular Activation Support for Cisco Catalyst Heavy Duty Routers	Specific pluggable interface modules of Cisco Catalyst IR8140 Heavy Duty Routers support the Managed Cellular Activation solution.
Cisco Catalyst SD-WAN Integrations	
Cisco Secure Equipment Access Integration	Cisco Secure Equipment Access (SEA) is a solution that provides remote access to network-connected assets. Assets can include anything reachable by IP address, such as servers, industrial internet of things (IIoT) devices, and so on. Integration with Cisco Catalyst SD-WAN enables you to use Cisco SD-WAN Manager to deploy the Cisco SEA solution within a Cisco Catalyst SD-WAN network.
Third-Party Custom Application Integration	Cisco SD-WAN Manager supports integration with third-party-developed Cisco IOx applications. These custom applications add functionality to devices that run Cisco IOSXE Catalyst SD-WAN software.

Software and Hardware Behavior Changes in Cisco Catalyst SD-WAN Manager Release 20.16.x

Software and Hardware Behavior Changes in Cisco Catalyst SD-WAN Manager Release 20.16.1

Behavior Change	Description
Cisco SD-WAN Manager deletes statistics files older than 14 days to prevent disk fill-up.	See the Onboard Cisco SD-WAN Analytics section.
The indicators about the health of a device. The following are the health status for edge devices: • Good: Edge device is using less than 80% of available memory, and less than 88% of CPU resources. • Fair: Edge device is using greater than equal to 80% of available memory, or 88% of CPU resources. • Poor: Edge device is using greater than equal to 90% of available memory, or 93% of CPU resources.	See the View Cisco SD-WAN Manager Status section.
The SHA-1 algorithm is disabled by default in Cisco SD-WAN Manager.	See the section SSH Encryption Algorithmsfor more details.

Behavior Change	Description
Cisco Cyber Vision integration support for Cisco Catalyst IR1800 Rugged Series	For Cisco Cyber Vision integration, added support for the Cisco Catalyst IR1800 Rugged Series. See Supported Platforms for Cisco Cyber Vision Integration.
Cisco Cyber Vision integration: token restriction	You can onboard a device in the network to Cisco Cyber Vision Center only one time using a single deployment token. See Restrictions for Cisco Cyber Vision Integration.
Cisco Cyber Vision integration: Moving devices from one Cyber Vision Center instance to another	If you have onboarded devices to an instance of Cisco Cyber Vision and you need to move them to a different instance of Cisco Cyber Vision, you need to first push a configuration to the devices that does not include the Cyber Vision feature. See Restrictions for Cisco Cyber Vision Integration.
Cloud gateway exemption from license requirement: No license is required for up to two Cisco 8000V devices if: • They are operating as cloud gateway routers for a Cisco SD-WAN Cloud Pro environment (Cisco cloud-hosted), and • They provide a gateway for a TACACS or syslog server located outside the Catalyst SD-WAN fabric. The license exemption requires tagging the devices with the Connector tag. After tagging the devices, the license compliance check will not flag them as requiring a license, and SD-WAN Manager will not show an out-of-compliance message for the devices.	

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.16.1a

Behavior Change	Description
The following show commands are no longer supported: • show sdwan from-vsmart policy • show sdwan from-vsmart tag-instances	See the show sdwan from-vsmart policy section.
The range for *instance id* in **l2vpn sdwan instance** command is 1 to 511 and 513 to 65527.	See the L2VPN Commands section for more details about this command.
The **Use Custom Commands** field does not support certain OMP and TTM show commands.	See the Generate Admin-Tech Files section for more details.

Behavior Change	Description
Configuring services using the **allow-service** *all* command on Cisco Catalyst SD-WAN Controllers is only applicable for the following services: **bgp**, **dhcp**, **dns**, **https**, **icmp**, **netconf**, **ntp**, **ospf**, **sshd**, and **stun**. Note that configuring **allow-service** *all* overrides any commands that allow or disallow individual services.	See the following sections for more details about this command: • allow-service command • Configure Adaptive QoS Using the CLI • Configure Implicit ACL on Loopback Interfaces Using CLI
The default OMP hold time is increased to 5400 seconds.	See the Configure OMP Timers section for more details.

Cisco Catalyst SD-WAN Manager Upgrade Paths

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

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

Table 3: Upgrade Paths For Cisco Catalyst SD-WAN Control Components Releases 20.6.x and Later Releases

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
20.6.x	Not Supported	Direct Upgrade	Direct Upgrade	Direct upgrade from 20.9.5.2 and later releases.	Step upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Step Upgrade from 20.15.1 and later releases. **Note** Ensure to complete the stats migration before you upgrade to version 20.16 For cluster upgrade procedure using CLI: **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

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
20.7.x	Not Supported	Not Supported	Direct Upgrade	Direct upgrade from 20.9.5.2 and later releases.	Step upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Step Upgrade from 20.15.1 and later releases. **Note** Ensure to complete the stats migration before you upgrade to version 20.16 For cluster upgrade procedure using CLI: **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-d diagnostic` command to chec the data base size. This is applicable only for upgrades of devices runnin Cisco SD-WAN

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
20.8.x	Not Supported	Not Supported	Not Supported	Direct upgrade from 20.9.5.2 and later releases.	Step upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Step Upgrade from 20.15.1 and later releases. **Note** Ensure to complete the stats migration before you upgrade to version 20.16 For cluster upgrade procedure using CLI: **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

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
20.9.x	Not Supported	Not Supported	Not Supported	Not Supported	Direct upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **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										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
								Direct upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** • We recommend the data base size in this 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. • If your Cisco	Direct Upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** • We recommend the data base size in this 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 from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** • We recommend the data base size in this 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. • If your Cisco	Step Upgrade from 20.15.1 and later releases. **Note** Ensure to complete the stats migration before you upgrade to version 20.16 For cluster upgrade procedure using CLI: **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

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
								Catalyst SD-WAN Manager running Cisco vManage Release 20.9.x and you are looking to upgrade to Cisco Catalyst SD-WAN Manager Release 20.12.x, we recommend you use the CLI mode of configuration for cluster upgrades. If Cisco Catalyst SD-WAN Manager is used for upgrading a cluster, the cluster's nms process fails when the new partition is activated. Continue to use the Cisco Catalyst SD-WAN Manager and CLI for standalone Cisco SD-WAN Manager upgrades.	Catalyst SD-WAN Manager Release 20.9.x and you are looking to upgrade to Cisco Catalyst SD-WAN Manager Release 20.12.x, we recommend you use the CLI mode of configuration for cluster upgrades. If Cisco Catalyst SD-WAN Manager is used for upgrading a cluster, the cluster's nms process fails when the new partition is activated. Continue to use the Cisco Catalyst SD-WAN Manager and CLI for standalone Cisco SD-WAN Manager upgrades.	Catalyst SD-WAN Manager Release 20.9.x and you are looking to upgrade to Cisco Catalyst SD-WAN Manager Release 20.12.x, we recommend you use the CLI mode of configuration for cluster upgrades. If Cisco Catalyst SD-WAN Manager is used for upgrading a cluster, the cluster's nms process fails when the new partition is activated. Continue to use the Cisco Catalyst SD-WAN Manager and CLI for standalone Cisco SD-WAN Manager upgrades.	Catalyst SD-WAN Manager Release 20.9.x and you are looking to upgrade to Cisco Catalyst SD-WAN Manager Release 20.12.x, we recommend you use the CLI mode of configuration for cluster upgrades. If Cisco Catalyst SD-WAN Manager UI is used for upgrading a cluster, the cluster's nms process fails when the new partition is activated. Continue to use the Cisco Catalyst SD-WAN Manager UI and CLI for standalone Cisco SD-WAN Manager upgrades.	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										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											• If your Cisc Catalyst SD-WAN Manager is running Cisc vManage Release 20.9.x and you are looking to upgrade to Cisco Catalyst SD-WAN Manager Release 20.12.x, we recommend you use the CLI mode o configuratio for cluster upgrades. If Cisco Catalyst SD-WAN Manager UI is used for upgrading a cluster, the cluster's nms process fails when the nev partition is activated. Continue to use the Cisc Catalyst SD-WAN Manager UI and CLI for standalone Cisco SD-WAN Manager upgrades.

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
20.10.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade	Direct Upgrade	Direct Upgrade	

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Step Upgrade from 20.15.1 and later releases. **Note** Ensure to complete the stats migration before you upgrade to version 20.16 For cluster upgrade procedure using CLI: **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-d diagnostic` command to chec the data base size. This is applicable only for upgrades of devices runnin Cisco SD-WAN

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
20.11.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade	Direct Upgrade	

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Step Upgrade from 20.15.1 and later releases. **Note** Ensure to complete the stats migration before you upgrade to version 20.16 For cluster upgrade procedure using CLI: **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

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
20.12.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade	

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Step Upgrade from 20.15.1 and later releases. **Note** Ensure to complete the stats migration before you upgrade to version 20.16 For cluster upgrade procedure using CLI: **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-d diagnostic` command to chec the data base size. This is applicable only for upgrades of devices runnin Cisco SD-WAN

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
20.13.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Step Upgrade from 20.15.1 and later releases. **Note** Ensure to complete the stats migration before you upgrade to version 20.16 For cluster upgrade procedure using CLI: **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

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
20.14	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Step Upgrade from 20.15.1 and later releases. **Note** Ensure to complete the stats migration before you upgrade to version 20.16 For cluster upgrade procedure using CLI: **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-d diagnostic` command to chec the data base size. This is applicable only for upgrades of devices runnin Cisco SD-WAN

Starting Cisco SD-WAN Manager Version	Destination Version										
	20.6.x	20.7.x	20.8.x	20.9.x ***	20.10.x ***	20.11.x ***	20.12.x ***	20.13.x ***	20.14.x ***	20.15.x ***	20.16.x ***
											Manager Release 20.1.1 and later.
20.15	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade **Note** We recommend using the GUI method via Cisco SD-WAN Manager to perform the upgrade.

Note * To check the free disk space using the CLI:

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

** The cluster upgrade must be performed using CLI.

- The **request nms configuration-db upgrade** upgrade procedure must be performed only on one node in the cluster.
- During the configuration-db upgrade process, 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.
- To upgrade the configration database and to determine the node that needs an upgrade, enter **request nms configration-db status** command on each of the nodes. In the output look for the following:

```
Enabled: true
Status: not running
```

Note After activating a new image on a Cisco SD-WAN Manager host server, the server reboots. After the reboot, for approximately 30 minutes, the output of the **request nms configuration-db status** command shows **Enabled: false** even on a node that has the configuration database enabled, while NMS services are being migrated to a containerized form. On the node to upgrade, as determined in the previous step, enter the following: **request nms configration-db upgrade**

*** After upgrading to version 20.9.5.2 or later, the statistics-DB version migration process may take up to 4 hours. It is crucial to ensure that the migration is complete before proceeding with subsequent steps.

Steps to Verify Migration Completion:

1. Execute Diagnostic Command:

   request nms statistics-db diagnostics

2. Check Diagnostic Output: Ensure that there are 0 entries under the section titled **"Indices with major version lesser than 6".** This indicates that the migration is complete.

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.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.16.x

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.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.16.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.16.1

Identifier	Headline
CSCwm51140	20.15.2: "adminresetrequired?component=configdb" API timing out on Cisco SD-WAN Manager UI.
CSCwm59794	Default values for variables name in config group aren't accepting more than 60 characters.
CSCwm84084	Web Server certificate migration failure to vault after upgrade.
CSCwm73117	Missing categories in Cisco SD-WAN Manager GUI running 20.12.4
CSCwm02422	Dashboard doesn't show the left navigation bar on Cisco SD-WAN Manager.
CSCwm04682	Cisco SD-WAN Manager: Certificate installation getting stuck when initiated from a Cisco SD-WAN Manager node in cluster setup.
CSCwm94648	Color Group getting removed after applying the AAR Policy to COR for SAAS.
CSCwk97594	Cisco SD-WAN Manager upgrade from 20.9.5.1 to 20.12.3 is failing with neo4j authentication failure.
CSCwk99319	Encapsulation value is not set on Traffic Engineering Policy on Cisco SD-WAN Manager 20.14.1
CSCwm68939	Customer migrated from 20.9.5 to 20.15.1 and all their devices are showing no license assigned.
CSCwm39910	Cisco SD-WAN Manager : License count mismatch between Cisco SD-WAN Manager & CSSM portal with Online reporting.
CSCwm77182	"All OSPF peering sessions are down" ghost alarm for the non-ospf routers.
CSCwm77677	Configuration Group: dual router feature parcel 'Save' issues.
CSCwm91051	20.15.1-390- Object tracker elements are not visible in VRRP after configuring.
CSCwm94803	Cisco SD-WAN Manager alarm - email notification setting doesn't allow upper case in the mail ID.
CSCwm43112	In Cisco SD-WAN Manager running 20.12.1 code, the DE registration was stuck in pending state for several days.
CSCwm87865	After shutting down the standby Cisco SD-WAN Manager and bringing them up, the DR replication is failing.
CSCwk55096	Policy Group: default application policy does not follow cisco validated design DSCP marking.
CSCwm32642	Unable to edit switchport feature template on Cisco SD-WAN Manager.

Identifier	Headline
CSCwk79993	[MRF] Region field is missing from the internal parcel while deploying the config-group.
CSCwm47780	Cisco SD-WAN Manager rejects SAML responses that include line breaks.
CSCwk66060	OMP extranet policy not exporting all the routes for the prefixes.
CSCwm61587	Configuration Group: not able to search configuration preview.
CSCwm70543	Device is displayed as 'Healthy' despite Missing 1+ expected Cisco SD-WAN Controller control connections.
CSCwm65713	Configuration Group: 'Back' Button in feature profile does not return to previous page.
CSCwk74774	Local user not able to login on Cisco SD-WAN Manager 20.12.3, auth-fall back fails when "priority" is configured.
CSCwm72199	The 'service local' is not pushed to WAN Edges after upgrade from 20.9.5 to 20.12.4.
CSCwm11883	Cisco SD-WAN Manager upgrade fails / upgrade pre-check script needs to be more descriptive.
CSCwm13281	Introduce transaction timeout in Neo4j.
CSCwm52650	Configuration group can not be pushed due to error duplicate tag name.
CSCwm79728	Configuration Group Deployment: Device variables not grouped together.
CSCwm91228	MTT: Tenant creation fails "Failed to create tenant".
CSCwm11848	Cisco SD-WAN Manager VPN templates corrupted after upgrade to 20.12.x
CSCwm61578	Configuration Group: Side by side preview has scrollbar for old and new configuration.
CSCwm44608	Cisco SD-WAN Manager Tools -> TAC cases fails DUO authentication.
CSCwk92103	Cisco NFVIS SD-Branch: 2nd device not upgrade in the same site-id after the 1st device is upgraded successfully.
CSCwk55953	Policy Group: Cloud OnRamp Gateway Service VPN only showing VPN 512 interfaces.
CSCwm36264	IPv6 prefix push template fails.
CSCwn06875	Configuration Group: Maximum IP MTU value for HundredGigE sub-Interface is 2000.
CSCwm07628	Not able to add new tracker while using generic on cisco secure internet gateway (SIG).
CSCwn12834	Neo4j/GUI is not coming up after virtual machine size upgrade.
CSCwm70614	Stats data not visible after upgrading to 20.12.3.1 MTT setup.
CSCwm09327	Wasted space in Policy Application page.

Identifier	Headline
CSCwe42844	Cisco IOS XE Catalyst SD-WAN device SNMPv3 feature template: Cannot create User with SHA-256 auth option.
CSCwk67930	Cisco SD-WAN Manager GUI becomes intermittently unavailable on 20.9.3 cluster in round robin fashion.
CSCwn03490	Cisco SD-WAN Manager processing all groups sent by SSO IDP resulting in delayed login.
CSCwk95312	Remove the unused docker default network.
CSCwm54703	20.9.4.1 Cisco SD-WAN Manager app-server restarted due to app-server OOM Java heap space.
CSCwk61793	After Applying SaaS, AAR Policy in the GUI differs from AAR Policy in the CLI.
CSCwm09265	Server names - Asterisk is not required for custom applications.
CSCwm67246	CLI Add-On: Encrypt Type6 password for wireless credentials not working.
CSCwm73952	Cisco SD-WAN Manager upgrade from 20.12.3.1 to 20.15.1 fails in post-upgrade-check-fail.
CSCwm74306	Configuration Group: Switchport Parcel has 802.1X on by Default.
CSCwm35064	High CPU utilization on multiple Cisco SD-WAN Manager cluster nodes randomly 20.9.5.2.7
CSCwm35108	Neo4j getting killled due to OOM resulting in GUI being unavailable even with enough resources.
CSCwk95942	OSPF MD5 Key is configured incorrectly on port-channel interfaces via configuration groups.
CSCwk66686	Cisco SD-WAN Manager NMS services do not start after upgrading from 20.9.3ES2 to 20.15EFT2
CSCwm60069	Configuration Group: Feature Parcels from Policy Profile are duplicated by copy function.
CSCwm27466	Cisco SD-WAN Manager: Warning message when customer configures allow-service all via config-grp and template.
CSCwm34478	Cisco SD-WAN Manager 20.12.x, filling variables in device templates with "#" causes corruption in CSV file.
CSCwk58441	Some sites which are active are not visible on CoR SaaS > Application page.
CSCwm46129	Cisco SD-WAN Manager is unable to process gracefully, when software installs tasks if they exceed 40 installations.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.16.1

Identifier	Headline
CSCwn19880	[20.12.4-590] DR: stats files not being processed in 2 standby nodes.
CSCwq91481	DR: Scale configuration causes neo4j to crash and restart in secondary when deleting & importing SYSTEMDEVICESNODE.
CSCwn18532	Cisco SD-WAN Manager - Configuration group service profile switchport not responding.
CSCwm88294	20.16 EFT: java.lang.NullPointerException while forming cluster.
CSCwn33502	Policy Group: 'Failed to deploy device with Policy Group' error due to dynamic VPN ID configuration.
CSCwm27276	Cisco SD-WAN Manager: Replication of statistics file causes service-proxy 503 UH & GUI goes unreachable.
CSCwn24493	Unable to Update Edited Copied Feature Template 'Default_BootStrap_Cisco_System_Template' on Cisco SD-WAN Manager.
CSCwn33483	Policy Group Deployment: Ambiguous 'Failed to deploy device with Policy Group' error message.
CSCwn05583	Solution: 20.15.2 unable to push Cisco SD-WAN Controller config different PG from Cisco SD-WAN Manager.
CSCwm85904	Cisco SD-WAN Manager: control policy is getting removed during configuration sync.
CSCwk60384	Controller establishes multiple viptela-device session and affects performance.
CSCwm14592	Cisco SD-WAN Manager UI Password create or update.
CSCwm72096	Unable to upgrade Cisco SD-WAN Validator via GUI from 20.14.1 to 20.15.1
CSCwn30415	Cisco SD-WAN Manager olap-db query_log bloated - 20.15.1
CSCwn36666	20.15 Switchover failed - Failed to push Cisco SD-WAN Controller list.
CSCwn05679	TAC case option in Cisco SD-WAN Manager does not redirect correctly.
CSCwn23134	Repllication for DR takes time after services on Cisco SD-WAN Manager restart.
CSCwn51068	After upgrading to 20.16 or later images, show reboot history is getting cleaned up
CSCwn50168	Upgrade from Cisco Catalyst SD-WAN Manager Release 20.15.x to 20.16 (or later) causes device to never come up when boot fs is ext*.
CSCwn51488	Multiple active user sessions exist on Cisco SD-WAN Manager even after controller upgrade transaction completes.
CSCwn50355	Certificate expiry date for Cisco Catalyst 8000V Edge Software is not displayed in the UI due to incorrect key.

Identifier	Headline
CSCwn68973	License management reporting section displays blank page in Cisco SD-WAN Manager GUI.
CSCwn62802	Remote circuit field is not resetting when updating the remote device.
CSCwo39530	Applied changes in the filter of pcap fileds are not reflecting after refreshing

Cisco Catalyst SD-WAN Manager API

For information on Cisco SD-WAN Manager Release 20.16.x APIs, see Cisco SD-WAN Manager API.

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)

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)

© 2024–2026 Cisco Systems, Inc. All rights reserved.