Release Notes for Cisco Catalyst SD-WAN Control Components Release 20.10.x

First Published: 2022-11-10

Last Modified: 2023-08-11

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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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 20.10.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**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. 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, Release 20.10.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 SD-WAN Devices, Cisco IOS XE Release 17.10.x.

What's New for Cisco Catalyst SD-WAN Control Components Release 20.10.x

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 IOS XE Release 17.10.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started Guide	
Updates to the SD-AVC Cloud Connector Login Process	Logging in to the Cloud Connector now requires a cloud gateway URL and a one-time password (OTP) instead of a client ID and client secret.
Cisco Catalyst SD-WAN Systems and Interfaces	

Feature	Description
Security Feature Profile in Configuration Groups	This feature allows you to configure Security Profile in the Configuration Groups.

Localized Policy Configuration for QoS, ACL, and Route Features	This feature allows you to configure Policy Object Profile in the Configuration Groups.
	The following enhancements are introduced in the Policy Configuration Group feature.
	• Policy Object Profiles
	  • AS Path
	  • Standard Community
	  • Expanded Community
	  • Data Prefix
	  • Extended Community
	  • Class Map
	  • Mirror
	  • Policer
	  • Prefix
	  • VPN
	• QoS MAP Policy under Service and Transport profiles
	• Route Policy under Service and Transport profiles
	• ACL Policy under Service and Transport profiles

Variables and Type6 Encryption in CLI Profile	After you enter or import configuration into a CLI profile, convert certain values to device-specific variables or encrypt strings such as passwords using Type6 encryption.
Secure SRST support on Cisco Catalyst SD-WAN	This feature provides support for additional CUBE commands that can be used in Cisco IOS XE Catalyst SD-WAN device CLI templates or CLI add-on feature templates, and qualifies selected Cisco Survivable Remote Site Telephony (SRST) commands for use with CLI templates in Cisco SD-WAN Manager.
DHCP Vendor Option Support	This feature allows DHCP client options, 124 and 125 to configure vendor-specific information in client-server exchanges. Configure this feature using the CLI Add-on feature template in Cisco SD-WAN Manager.

Feature	Description
IPv6 as Preferred Address Family in a Dual Stack Environment	This feature allows you to select IPv6 as the preferred address family for control and data connections in a dual stack network environment. For Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller, configure IPv6 as the preferred address family by using the feature template or the CLI template. For Cisco IOS XE SD-WAN devices, configure IPv6 as the preferred address family using the Configuration Groups, Quick Connect or a CLI template.
Bulk API Rate Limit for a Cisco SD-WAN Manager Cluster	For a Cisco SD-WAN Manager cluster, the rate limit for bulk APIs equals (rate-limit per node) * (number of nodes in the cluster). Cisco SD-WAN Manager distributes bulk API requests among the nodes in the cluster. With these changes, you can retrieve data faster from a Cisco SD-WAN Manager cluster through bulk APIs.
Network Hierarchy and Resource Management (Phase II)	The following enhancements are introduced in the Network Hierarchy and Resource Management feature. • Creation of a system IP pool on the **Configuration** > **Network Hierarchy** page • Automatic assignment of site ID, system IP, and hostname to a device in the Quick Connect workflow • Display of detailed information on the **Configuration** > **Network Hierarchy** page, including site ID pool, region ID pool, and the list of devices associated with a site
Cisco Catalyst SD-WAN Routing	
Automatically Suspend Unstable Cisco Catalyst SD-WAN BFD Sessions	With this feature, you can automatically suspend an unstable Cisco Catalyst SD-WAN Bidirectional Forwarding Detection (BFD) session based on flap-cycle parameters or on Service-Level Agreement (SLA) parameters. You can also monitor the suspended BFD sessions and manually reset suspended BFD sessions.
Cisco Catalyst SD-WAN Policies	
Flexible NetFlow Export of BFD Metrics	With this feature, you can export Bidirectional Forwarding Detection (BFD) metrics to an external collector for generating BFD metrics of loss, latency, and jitter. This feature provides enhanced monitoring and faster collection of network state data. After you enable export of BFD metrics, configure an export interval for exporting the BFD metrics.
Real-Time Device Options for Monitoring Cflowd and SAIE Flows	With this feature, you can apply filters for monitoring specific Cflowd and Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) applications or application families running within a VPN on the selected Cisco IOS XE Catalyst SD-WAN device. Real-time device options for monitoring Cflowd and SAIE flows are available on Cisco vEdge devices. This release provides support for monitoring Cflowd and SAIE applications on Cisco IOS XE Catalyst SD-WAN devices.

Feature	Description

Lawful Intercept 2.0 Enhancements	• Cisco SD-WAN Manager GUI enhancements:
	  • A **Sync to vSmart** button to synchronize a newly created intercept configuration with the Cisco Catalyst SD-WAN Controller.
	  • A toggle button to enable or disable an intercept.
	  • A progress page to display the status of the synchronization and activation.
	  • A red dot on the Task-list icon in the Cisco SD-WAN Manager toolbar to indicate any new Lawful Intercept tasks.
	  • A Task list side bar to view a list of active and completed Lawful Intercept tasks.
	  • An intercept retrieve option **Get IRI** to retrieve key information or Intercept Related Information (IRI) from the Cisco Catalyst SD-WAN Controller.
	• Ability to troubleshoot Cisco SD-WAN Manager and Cisco SD-WAN Manager using the debug logs and using admin tech files.

Cisco Catalyst SD-WAN Security	
Cisco Catalyst SD-WAN Identity-Based Firewall Policy Enhancement for SGT Integration	The Cisco Catalyst SD-WAN identity-based firewall policy feature is enhanced to support Security Group Tag (SGT) integration with ISE. SGTs are assigned in networks to simplify policy configuration across devices.
IPS Custom Signature and Offline Updates	This feature lets you download UTD signature packages for the Intrusion Prevention System (IPS) out of band from Cisco.com and upload these packages to Cisco SD-WAN Manager or a remote server for Cisco SD-WAN Manager to distribute. It also lets you upload a custom signature rules file to Cisco SD-WAN Manager or a remote server, which Cisco SD-WAN Manager then distributes and appends to the existing UTD signature package rules.
Configure SIG Tunnels in a Security Feature Profile	With this feature, create a Security feature profile and associate it with one or more configuration groups. In the Security feature profile, configure the Secure Internet Gateway feature to create automatic or manual SIG tunnels. After configuring the feature, deploy the configuration group on the desired WAN edge devices to create SIG tunnels from the devices to the configured SIG endpoints.
Configure Multiple IdPs for Single Sign-On Users of Cisco SD-WAN Manager	With this feature, you can configure up to three IdPs for providing different levels of access for single sign-on users of Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN Cloud OnRamp	

Feature	Description
Improved Visibility and Control of Webex Traffic	This feature introduces several improvements to the visibility and control of Webex traffic, including the following: • Using Cisco SD-AVC to manage deep packet inspection (DPI) of Webex traffic • Receiving server-side Webex metrics to provide detailed information about Webex traffic performance • Adding only a single sequence to control policies to enable Cloud OnRamp for SaaS for Webex traffic
Monitoring MultiCloud Services for Real Time Data in Cisco SD-WAN Manager	This feature provides enhancements to monitoring dashboard for all the Cloud and Interconnect connections. This feature also gives you the flexibility to specify which dashlets to view and sort them based on your preferences.
Modify Additional Properties of Interconnect Connections to AWS and Microsoft Azure	Interconnect Connections to AWS: • Cisco vManage Release 20.9.x and earlier: You can edit only the bandwidth of a hosted VIF connection after it is created. Properties of hosted connections cannot be edited after connection creation. With this feature, edit additional properties of both hosted VIF and hosted connections after connection creation. • Cisco vManage Release 20.9.x and earlier: You cannot edit a VPC tag that is associated with a connection. With this feature, to attach VPCs to or detach VPCs from a Private Hosted VIF, Private Hosted Connection, or a Transit Hosted Connection, edit the VPC tags associated with the connection to add or remove VPCs. Interconnect Connections to Microsoft Azure: • Cisco vManage Release 20.9.x and earlier: You can edit only the bandwith of a connection after it is created. Other properties of a connection are not editable. With this feature, edit additional properties of both Microsoft peering and private peering connections. • Cisco vManage Release 20.9.x and earlier: You cannot edit a VNet tag that is associated with a connection. With this feature, to attach VNets to or detach VNets from a Private Peering Connection, edit the VNet tags associated with the connection to add or remove VNets.
Cisco Catalyst SD-WAN Monitor and Maintain	
Applications Performance and Site Monitor	You can monitor and optimize the application health and performance on all sites or a single site using Cisco SD-WAN Manager.

Feature	Description
Reports	Reports provide a summarized view of the health and performance of the sites, devices, and tunnels in your network. You can schedule a report, download it as a PDF document, and receive it as an email. The **Reports** menu has been added to Cisco SD-WAN Manager.
Remote Server Support For ZTP Software Upgrades	This features introduces remote server support for upgrading the software of the Cisco IOS XE Catalyst SD-WAN Devices in scale using Zero Touch Provisioning (ZTP). The software upgrade images are uploaded to Cisco SD-WAN Manager using a preferred remote server and the respective devices are upgraded.
Improved Access to Troubleshooting Tools in Cisco SD-WAN Manager	The troubleshooting tools are now easily accessible from various monitoring pages of Cisco vManage, such as **Site Topology**, **Devices**, **Tunnels**, and **Applications**, thereby providing you context-based troubleshooting guidance. Earlier, the troubleshooting tools were accessible only from the device dashboard.
Speed Test Support	This feature enables you to carry out speed testing and evaluate the bandwidths on Cisco IOS XE Catalyst SD-WAN devices and iperf3 servers.
Time Filter in Monitor Overview and Monitor Security Dashboards in Cisco vManage	The time filter option added to the **Monitor Overview** and **Monitor Security** dashboards in Cisco SD-WAN Manager enables you to filter the dashboard data for a specified time range.
Underlay Measurement and Tracing Services	The underlay measurement and tracing services (UMTS) feature provides visibility into the paths that tunnels take between local and remote Cisco IOS XE Catalyst SD-WAN Devices, through the underlay network (the physical devices that compose the network). For a specific tunnel, the path includes all nodes between the two devices. You can enable UMTS using Cisco SD-WAN Manager. You can view the resulting path information in Cisco SD-WAN Manager and in Cisco vAnalytics.
Software Upgrade Scheduling Support for Additional Platforms	Added support for software upgrade scheduling for Cisco Catalyst Cellular Gateways and Cisco Catalyst Wireless Gateways.
Cisco Catalyst SD-WAN NAT	
Support for Source Port Preservation for well-known SD-WAN Ports	This feature allows preservation of well-known SD-WAN ports during NAT.
Mapping of Address and Port Using Encapsulation (MAP-E) with NAT64	This feature provides support for an IPv4 client to access IPv4 servers when using an IPv6-only network. IPv4 traffic is routed to the internet over an IPv6 tunnel. With this feature, you can configure a MAP-E domain and MAP-E parameters for transporting IPv4 packets over an IPv6 network using IP encapsulation. When the MAP-E customer edge (CE) device starts or when an IPv4 address changes, the device obtains the MAP-E parameters automatically from the MAP-E rule server using HTTP.
Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)	

Feature	Description
Multi-Region Fabric Subregions	You can create subregions within an access region. Subregions enable you to separate edge routers into multiple distinct domains.
Multi-Region Fabric Using Multicloud and SDCI	This feature enables you to configure a cloud backbone or a Software-Defined Cloud Interconnect (SDCI) provider backbone as core region (region 0), and cloud gateways or interconnect gateways as border routers. You can thus easily establish site-to-site connectivity in multiple cloud regions and cloud networks.
Subregions in Policy	Subregions are defined domains within access regions. You can specify subregions when creating region lists, configuring policy, and applying policy.
Enhancements to Match Conditions	When configuring match conditions for policy, you can specify to match to all access regions, or to match according to a subregion.
Migrate a BGP-Based Hierarchical Core Network to Multi-Region Fabric	This feature facilitates migrating a BGP-based hierarchical core network into a Cisco SD-WAN Multi-Region Fabric-based topology by alleviating the need of complex control policy definitions and the existence of a BGP core.
Cisco Catalyst SD-WAN CloudOps	
Multitenancy Support on Microsoft Azure	Multitenancy Support for Cisco SD-WAN Control Components on Microsoft Azure.
Cisco IOS XE Catalyst SD-WAN Qualified Command Reference	
CLI Hardening Commands on Cisco IOS XE SD-WAN devices	CLI Hardening commands are added in AAA Commands Line Commands Logging Commands SNMP Commands

Important Notes, Known Behaviors, and Workarounds

- If your ConfigDB (Neo4j) username contains a – (hyphen), the ConfigDB upgrade fails, for example, db-admin. Remove the hyphen before you upgrade the ConfigDB.
- From Cisco SD-WAN Release 20.4.1.1, the Microsoft Azure environment is supported for deploying Cisco SD-WAN controllers (Cisco vBond orchestrator, Cisco vSmart controller, and Cisco vManage). The support is limited to Cisco SD-WAN cloud-based deployments only.
- From Cisco Catalyst SD-WAN Control Components Release 20.10.1, support for IPv6 is provided for the following features:
  - AWS and Azure cloud deployments
  - Cisco Smart Licensing
  - DNS

- NTP
- RADIUS
- SNMP
- Syslog
- TACACS+

- Your Cisco vManage needs to run Cisco vManage Release 20.9.1, if you want to upgrade to Cisco vManage Release 20.10.1. You can't upgrade directly to Cisco vManage Release 20.10.1 from Cisco vManage Release 20.7.1 and Cisco vManage Release 20.8.1.
- If you are upgrading Cisco vManage in clusters from Cisco SD-WAN Controllers Release 20.9.x to 20.10.x, the configuration database might be empty. Starting from Cisco SD-WAN Controllers Release 20.10.x, the configuration database version is upgraded to 4.4.5 from 4.1.1. Here are the instructions to upgrade the configuration database manually:

  1. Ensure that you have a snapshot or backup of the database that you are going to update using the following command:

     ```
     device# request nms configuration-db backup path <file-name>
     ```
  2. Install the Cisco vManage image binaries to the nodes of the cluster that you want to upgrade using the following command:

     ```
     device# request software install <path>
     ```

Note Install the image and do not activate.

  3. Stop NMS services on all the Cisco vManage cluster nodes using the following command:

     ```
     device# request nms configuration-db stop
     ```
  4. Activate the image binaries on each of the Cisco vManage node in the cluster using the following command:

     ```
     device# request software activate <version>
     ```
  5. Upgrade the configuration database on any one of the nodes in the cluster that has the configuration database enabled using the following command:

     ```
     device# request nms configuration-db upgrade
     ```

  The configuration database (config-db) is now upgraded to the version 4.4.5.

- When using Cisco Catalyst SD-WAN Control Components Release 20.10.x or later, in a Cisco-hosted installation of Cisco Catalyst SD-WAN, the SD-AVC components operate differently than in earlier releases. Consequently, running the **request nms all status** command on the Cisco Catalyst SD-WAN instance shows that the "NMS SDAVC server" component is not enabled. This is expected behavior, and does not indicate any problem with SD-AVC. Note that the "NMS SDAVC gateway" component shows as enabled.

Cisco SD-WAN Manager Upgrade Paths

For information about Cisco SD-WAN Manager upgrade procedure, see Upgrade Cisco SD-WAN Manager 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	20.7.x	20.8.x	20.9.x	20.10.x
18.x/19.2.x	Direct Upgrade	Direct Upgrade		Step upgrade through 20.3.x	Step upgrade through 20.3.x 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 through 20.3.x 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 through 20.3.x 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 through 20.3.x 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 through 20.3.x 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 20.6.x or 20.9.x 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									
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x
			Check disk space* • If the disk space is more than 2 GB, Direct Upgrade • If the disk space is less than 2 GB, Step upgrade through 20.1 • If you are upgrading to 20.5, the available disk space should be at least 2.5 GB. For 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	20.7.x	20.8.x	20.9.x	20.10.x
			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									
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x
20.1.x	Not Supported	Not Supported	Direct Upgrade 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 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 through 20.3.x 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 through 20.3.x 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 through 20.3.x 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 through 20.3.x 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 through 20.3.x 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 20.6.x or 20.9.x 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									
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x
20.3.x	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade 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 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 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 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 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 20.6.x or 20.9.x 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									
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x
20.4.x	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade 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 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 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 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 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 from 20.6.x or 20.9.x 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	20.7.x	20.8.x	20.9.x	20.10.x
20.5.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade	Direct Upgrade	Step upgrade from 20.6.x or 20.9.x For cluster upgrade procedure: **request nms configuration-db upgrade** **Note**

We re
the da
in the
than c
5GB.
reque
confi
diagr
comm
the da
This i
only f
of dev
Cisco
Mana
20.1.1

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	20.7.x	20.8.x	20.9.x	20.10.x
20.6.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade	Step upgrade from 20.6.1, 20.6.2, and 20.6.3 either to 20.6.4 or 20.9.x. or Direct upgrade from 20.6.4 and later releases. For cluster upgrade procedure: **request nms configuration-db upgrade** **Note**

We recon
the data b
in the dis
than or e
5GB. Use
`request`
`configur`
`diagnost`
command
the data b
This is ap
only for u
of device
Cisco SD
Manager
20.1.1 an

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	20.7.x	20.8.x	20.9.x	20.10.x
20.7.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Step upgrade from 20.9.x For cluster upgrade procedure: **request nms configuration-db upgrade** **Note**

We re
the da
in the
than c
5GB.
`reque`
`confi`
`diagn`
comm
the da
This i
only f
of dev
Cisco
Mana
20.1.1

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	20.7.x	20.8.x	20.9.x	20.10.x
20.8.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Step upgrade from 20.9.x For cluster upgrade procedure: **request nms configuration-db upgrade** **Note**

We recon
the data b
in the dis
than or e
5GB. Use
`request`
`configur`
`diagnost`
comman
the data b
This is ap
only for u
of device
Cisco SD
Manager
20.1.1 an

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	20.7.x	20.8.x	20.9.x	20.10.x
20.9.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct upgrade For cluster upgrade procedure: **request nms configuration-db upgrade** **Note**

We re
the da
in the
than c
5GB.
reque
confi
diagr
comm
the da
This i
only f
of dev
Cisco
Mana
20.1.1

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

- The cluster upgrade procedure must be performed only on one node in the cluster
- 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.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.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.10.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 20.10.1.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.10.1.2

Identifier	Headline
CSCwf76218	Cisco Catalyst SD-WAN Manager Unauthenticated REST API Access Vulnerability.
CSCwf82344	Cisco Catalyst SD-WAN Manager Unauthenticated REST API Access Vulnerability.
CSCwf68936	Cisco SD-WAN vManage Authorization Bypass Vulnerability
CSCwf55823	Cisco Catalyst SD-WAN Manager Authorization Bypass Vulnerability

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.10.1.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.10.1.1

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

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.10.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.10.1

Identifier	Headline
CSCwc51421	20.10 : nested feature profile RBAC is not handled properly
CSCwc08313	System does not throw an error message for the overlapping policies in some cases.
CSCwd21136	UX2.0:20.9: VPN0-MGMT-VPN parcel IPv4 Static Route GW set to "Default" deploy failed
CSCwc13452	Memory leak in Cisco SD-WAN Controllers-OMP
CSCwc43513	Stats are not getting processed on Cisco SD-WAN Manager GUI running 20.8.1 code
CSCwd52180	UX2.0/20.10: Cisco SD-WAN Manager BGP parcel truncates "0" when we use BGP AS dot notation.
CSCwb37779	UX2.0: LAN Segment: Created two intf asso. the same VPN, device specific variables are duplicated
CSCwd20179	Devices not able to perform upgrade when data collection is turned off as site-id is not known.

Identifier	Headline
CSCwb91298	SD-AVC Cloud Connector Error alarm(possible_causes: CREDENTIALS) is not cleared
CSCwc60902	MTT Unreachable device not showing up in common inventory page
CSCwb68441	VPN drop menu shows empty in NWPI when we iniiate trace for first time
CSCwd33057	Cisco SD-WAN Manager upgrade failed from 20.6 build 20.9 due to nms app-server service restarts continously
CSCwc70086	The side by side CLI compare does not put empty lines to see impact of change between 2 devices
CSCwb91924	Cisco SD-WAN Manager 20.8.1 "Error in generating configuration diff for the device" template with SIP commands
CSCwc55684	Cisco SD-WAN SIG GRE: Layer 7 Health check doesn't work on Loopback interfaces
CSCwb23030	Cisco SD-WAN Manager GUI takes a long time to load when using Firefox
CSCwd05854	Error in Cisco SD-WAN Manager when trying to "Sync Licenses and Refresh Devices
CSCwd21774	Saving WAN/LAN BGP parcel fails when BGP ipv4/ipv6 neighbor remoteAS is set to Global integer value
CSCvy72764	services still communicate via old OOB IP after changing the vpn 0 OOB interface IP
CSCwc71437	Controller group is not updated correctly when pushed from Cisco SD-WAN Manager
CSCwc75057	Cisco SD-WAN Manager configuration commit hit Aborted: application communication failure error
CSCwc72609	Incorrect behavior for ICMP redirect Disable from WAN/LAN interface parcel
CSCwa77149	API call /dataservice/statistics/dpi/aggregation returns error 500
CSCwc65025	Email Notifications failing when Security is set as TLS with Gmail SMTP
CSCwd78294	Screen goes into loading when logged in as a basic user
CSCwc05127	Breakdown of U-Plane communication after updating Cisco SD-WAN Controllers's CiscoPKI certificate
CSCwc65129	Cisco SD-WAN API docs are showing wrong json payload example for call /certificate/device/invalidate
CSCwc73492	20.10, Cisco vBond Hostname "NULL"
CSCwb73769	20.9: 60K lines centralized policy with 12 Cisco SD-WAN Controllerss taking ~3 hours for activation
CSCwc55697	exception handling in Cisco SD-WAN Manager code does not return details about the exception we are hitting

Identifier	Headline
CSCwb92586	20.3.4, DR Registration Failed
CSCwc32615	Cisco SD-WAN Manager 20.6.2.1 rootfs.rw/var/crash/ incrementing
CSCwc24241	Navigation to cancel from template "Confirm Load Method" popup does not cancel the operation
CSCwc81937	Cisco SD-WAN Manager has extra Netconf Sessions when making API calls
CSCwd28214	Test the AAR policy for ipv6 using Cisco SD-WAN Manager - UI related issue
CSCvz70097	Cisco SD-WAN Manager DSPFarm CUCM Template Dialog UI issues
CSCwc41119	Duplicate Role descriptors found in IDP metadata
CSCwd31527	Cisco SD-WAN Manager disaster recovery status on CLI is broken
CSCwa68925	20.3.4 -- 2 minutes delay in Webhook event.
CSCwc51414	Hide the options from workflow side menu for the config group which are hidden in workflow page
CSCwc59497	services still communicate via old OOB IP after changing the vpn 0 OOB interface IP(Ref CSCvy72764)
CSCwc08514	Cisco SD-WAN Manager GUI and CLI has different syntax for usergroup
CSCwd11782	UX2.0:20.9: LAN VPN10-99-Intf v4/v6 sec addr device specific variable giving dup'd names
CSCwb52667	Multiple selection fr dropdown list to maintain the order in AAA Server Auth order field
CSCwc59865	Cisco SD-WAN Manager statistics-db heap-dump and thread-print commands are not supported
CSCwd35596	Disaster Recovery warning shown when pushing templates to WAN Edge Devices
CSCwd37119	No Real Time Data or CPU/Memory data from ESR-6300-NCP-K9 17.9.1
CSCwd04623	Packet Capture: VPN 65530 is not letting the loopback 65530 to be chosen
CSCwd73714	Cisco SD-WAN Manager : DSPFarm template error while configuring "CUCM Media Resource Name"
CSCwb95806	botocore.errorfactory.RegionDisabledException when doing VPC discovery with some regions inactive
CSCwb97349	Cisco SD-WAN Manager GUI is not showing accurate information of ISR4K FAN module
CSCwc47669	Cisco SD-WAN Manager cannot edit ZBFW policy
CSCwb91858	some template integer fields can be changed using the scroll wheel

Identifier	Headline
CSCwc95869	Memory leak observed when adding a new node to a cluster
CSCwd23369	Standby Cluster configuration is lost during data replication
CSCwc95935	DCA.py to remove the check for vanalytics to push telemetry data
CSCwa79824	Cisco SD-WAN Manager alarms logs are not cleared upon clicking "Mark All as viewed" when notification is 999+
CSCwc65037	MRF: ompd crash in access Cisco SD-WAN Controllerss while running policy cases in regression
CSCwc50308	Frequent GC causing Server Unavailable returing 503, GUI unaccessible intermittently
CSCwc80099	After configdb credentials change, app-server is not coming up due to use of hyphen in credentials
CSCwd23143	MT-DR: Unregister DR failed, UI time out; API on both cluster shown DR is still enabled.
CSCwc87356	Cisco SD-WAN Manager "Renew Device CSR" task cannot be opened under completed tasks
CSCwc37072	Security template create failed with auth variable
CSCwc75127	Cisco SD-WAN Manager Cisco IOS XE Catalyst SD-WAN device BGP Summary Counts Are Incorrect
CSCvz62234	Cisco Catalyst SD-WAN Manager Unauthorized Configuration Rollback Vulnerability

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.10.1

Identifier	Headline
CSCwd07860	Cisco SD-WAN Manager is redirecting to wrong IDP when same domains are used in a certain order.
CSCwd31522	20.10 :Edit of single VPC fails to do mapping as required
CSCwb58176	SSO/ciscotacro/rw User Session invalidated when browser switches between Cisco SD-WAN Manager nodes in cluster
CSCwd62984	OMPD crashed in Cisco SD-WAN Controllers on ISE config removal
CSCwd44445	on Powering off one VM of the cluster GUI of rest of the two nodes not available
CSCwc66840	17.9 Config Preview for very large sec policy is taking too long compared to previous releases
CSCwd39502	Table view of template variable inputs show input values listed in a random order after upgrade

Identifier	Headline
CSCwd52998	Nutella migration should not be allowed if there is a config-group associated with the router

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.

Cisco SD-WAN Manager API

For information on Cisco vManage Release 20.10.x APIs, see Cisco vManage Release 20.10 API. For information on APIs added, modified, deprecated, or removed in Cisco vManage Release 20.10.x, see Cisco vManage Release 20.10 API Change Log.

Related Documentation

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

Full Cisco Trademarks with Software License

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)