Release Notes for Cisco Catalyst SD-WAN Control Components Release 20.11.x

First Published: 2023-04-06

Last Modified: 2023-07-17

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

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 20.11.x

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

These release notes accompany the Cisco SD-WAN Control Components, Release 20.11.x, which provides Cisco Catalyst SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager as applicable to Cisco SD-WAN Manager.

Related Releases

For release information about Cisco IOS XE Catalyst SD-WAN devices, refer to Release Notes for Cisco IOS XE Catalyst SD-WAN devices, Cisco IOS XE Catalyst SD-WAN Release 17.11.x.

What's New for Cisco Catalyst SD-WAN Control Components Release 20.11.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 Catalyst SD-WAN Release 17.11.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started Guide	
Support for Specifying Any Organization for WAN Edge Cloud Device Enterprise Certificates	When configuring controller certificate authorization for enterprise certificates on WAN edge cloud devices, you can specify any organization in the **Organization** field. You are not limited to organization names such as **Cisco Systems**. This feature enables you to use your organization's certificate authority name or a third-party certificate authority name.
SMU Support for Cisco ISR1100 and ISR1100X Series Routers	Added SMU support for Cisco ISR1100 and ISR1100X Series Routers.
Cisco Catalyst SD-WAN Systems and Interfaces	

Feature	Description
Cisco Catalyst SD-WAN Remote Access Configuration	This feature enables you to configure a remote access feature in system profile of the configuration groups. You can configure the following remote access parameters in system profile–Private IP Pool, Authentication, AAA Policy, IKEv2 Setting, and IPSec Settings.
Device Variable Option	This feature enables you to read or write variables from the Associate Devices page while deploying the devices.
Configuration Groups and Feature Profiles	The following new features are introduced to the Configuration Groups and Feature Profiles–Cisco Security in System Profile, IPV4-Device-Access-Policy in System Profile, IPV6-Device-Access-Policy in System Profile, OSPF Routing in Transport Profile, VPN Interface GRE in Transport Profile, IPSEC in Transport Profile, Tracker Group in Transport Profile, GPS in Transport Profile, IPSEC in Service Profile, Tracker in Service Profile, Tracker Group in Service Profile, UCSE in Other Profile, AppQoE in Other Profile, Remote Access feature in System Profile.
Support for Software Defined Remote Access Pools	Remote access refers to enabling secure access to an organization's network from devices at remote locations. The resource pool manager manages the IPv4 and IPv6 private IP address pools for Cisco Catalyst SD-WAN remote access devices. You can create a software defined remote access pool using the **Configuration** > **Network Hierarchy** page.
TLOC Extension Over IPv6	This feature enables the support of TLOC extension for IPv6.
GRE-in-UDP	This feature enables you to configure GRE-in-UDP tunnel.
Assigning Roles Locally to a User Defined by an Identity Provider for SAML SSO	If you are using an identity provider, such as Okta, for security assertion markup language (SAML)-based single sign-on (SSO), then you can define user roles through the identity provider. This feature enables you to assign user groups locally in Cisco SD-WAN Manager, when no roles are defined for the user by the identity provider.
Cisco Catalyst SD-WAN Policies	
Log Action for both Localized and Centralized Data Policies	With this feature, you can set log action parameter for data policy, application route policy and localized policy while configuring data policies on Cisco IOS XE Catalyst SD-WAN devices. The log parameter allows packets to get logged and generate syslog messages. Logs are exported to external syslog every five mins when flow is active. Logs are exported to external syslog server only when one is configured in the system, or else only console logging is done. Policy logs further can be controlled as per the configured rate. A new command **policy log-rate-limit** is introduced to support this feature.
QoS for Router Generated Cisco SD-WAN Manager Traffic	This feature helps you to prioritize or queue router-generated Cisco SD-WAN Manager traffic based on your specific requirements. Achieve routing vManage traffic through a queue of your choice using QoS policies and configuring class maps.
Cisco Catalyst SD-WAN Security	

Feature	Description
IPv6 Support for Zone-based Firewall	This feature adds support for configuring IPv6 Zone-based Firewall (ZBFW) in addition to the existing IPv4 ZBFW.
Security Logging Enhancements	This feature allows you to configure up to four destination servers to export the logs, and an option to specify a source interface for high-speed logging (HSL). The IP addresses for the destination servers can be IPv4, IPv6, or both.
Security Logging Enhancements	This feature enhances the capability of UTD logging in a unified security policy. When you configure UTD logging for exporting the UTD logs to an external syslog server, you can now specify the source interface from where the UTD syslog originate from.
Cisco Umbrella Multi-Org Support	This feature supports management of multiple organizations through a single parent organization. With this feature, Cisco Catalyst SD-WAN and umbrella for SIG supports different security policy requirements for different regions of the Cisco Catalyst SD-WAN network.
Cisco Catalyst SD-WAN Cloud OnRamp	
Support for Multiple Virtual Hubs per Region	You can create multiple virtual hubs in a single Azure region.
Audit Management	The audit management feature helps in understanding if the interconnect cloud and provider connection states are in sync with the Cisco SD-WAN Manager connection state. The State refers to the various connection statuses that Cisco SD-WAN Manager establishes with cloud services and providers. The audit helps in identifying the gaps or disconnects between Cisco SD-WAN Manager intent and what is realized in the cloud.
Cisco Catalyst SD-WAN Monitor and Maintain	
Security Dashboard Enhancements	This features introduces enhancements to the security dashboard in Cisco SD-WAN Manager. The security dashboard introduces a drop-down list **Actions** that enables you to edit the security dashboard and reset the security dashboard to the default view when you have modified the security dashboard, view the **SecureX** ribbon once it is configured. Additionally, you can access the Cisco Talos portal from Cisco SD-WAN Manager. A hyperlink of the Cisco Talos portal is added to the security dashboard.
SCM Integration Improvements	With this feature, you can access Support Case Manager (SCM) wizard using Cisco SD-WAN Manager. You can create, view, or edit the support cases directly from Cisco SD-WAN Manager without having to go to a different Case Manager portal.

Feature	Description
Grouping of Alarms	Alarms are filtered and grouped for devices and sites based on severity. View alarm details for a single site in the **Overview** dashboard. View alarms for a particular device by clicking the … icon in the **Monitor** > **Devices** window. View the top five alarms for a particular site in the **Monitor** > **Overview** window by choosing the **Site Topology** view icon and clicking the site. The **Related Event** column is added to the alarms filter.
Grouping of Events	Events are filtered and grouped based on severity for devices and sites. View events for a particular device by clicking the … icon in the **Monitor** > **Devices** window. View the top five events for a particular site in the **Monitor** > **Overview** window by choosing the **Site Topology** view icon and clicking the site.
Automatically Determine File Attributes for a Remote Virtual Image File	When you specify a remote virtual image file, Cisco SD-WAN Manager can extract the necessary image file attributes from the filename.
Unified Debug Condition To Match IPv4/IPv6 Over MPLS	This feature introduces a debug condition to identify and resolve issues related to matching IPv4/IPv6 traffic over an MPLS network.
Packet Trace Improvements	This feature offers the following enhancements to packet trace: • A new command **how platform packet-trace fia-statistics**, available on Cisco IOS XE Catalyst SD-WAN devices, displays Feature Invocation Array (FIA) statistics in a packet trace. In FIA statistics, you can find data about a feature's count, the average processing time, the minimum processing time, and the maximum processing time. • View label information for the Multiprotocol Label Switching (MPLS) feature in packet trace.
Download Output of OMP Routes	You can download the output of the OMP Received Routes or OMP Advertised Routes real time commands on Cisco IOS XE Catalyst SD-WAN device.
Cisco Catalyst SD-WAN SNMP	
Application Route SNMP Trap	Cisco IOS XE Catalyst SD-WAN device support the **AppRouteSlaChange** SNMP trap which is generated when a change in SLA class is detected.
Cisco Catalyst SD-WAN NAT	
Destination NAT Support	This feature changes the destination address of packets passing through WAN edge devices. Destination NAT is used to redirect traffic destined to a private address to the translated destination public IP address.

Feature	Description
Port Forwarding with NAT DIA Using a Loopback Interface	This feature supports port forwarding with NAT DIA by using a loopback interface. You can configure a loopback interface by either using device CLI templates or CLI add-on feature templates.
ALG Support Enhancement for NAT DIA and Zone-Based Firewalls	The ALG support for NAT DIA is extended for the following protocols–Trivial File Transfer Protocol (TFTP), Point-to-Point Tunneling Protocol (PPTP), Sun Remote Procedure Call (SUNRPC), Skinny Client Control Protocol (SCCP), H.323.
Support for IPv6 DIA Tracker	NAT DIA tracker is now supported on IPv6 interfaces. You can configure IPv6 DIA tracker using the **IPV6-Tracker** and **IPV6-Tracker Group** options under transport profile in configuration groups.
Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)	
Support for Affinity Groups for Service Routes and TLOC Routes	This feature extends support affinity group assignments to service routes and TLOC routes. A common use case is to add further control to routing by using affinity group preference together with control policies that match service routes and TLOC routes.
Set Affinity Group by Control Policy	You can configure a control policy to match specific TLOCs or routes and assign them an affinity group value, overriding the affinity group that they inherit from the router.
Route Aggregation on Border Routers and Transport Gateways	With this feature, you can configure route aggregation on border routers and transport gateways in a Multi-Region Fabric network environment. For a border router, you can optionally specify whether the route aggregation operates only for the router's core region or access region.
Cisco Catalyst SD-WAN Routing	
Support for MSDP to Interconnect Cisco Catalyst SD-WAN and Non-SD-WAN	This feature enables Multicast Source Discovery Protocol (MSDP) interoperability between Cisco IOS XE Catalyst SD-WAN devices in Cisco Catalyst SD-WAN and the devices in a non-SD-WAN setup.
Cisco SD-WAN Controller Route Filtering by TLOC Color	Cisco SD-WAN Controller can reduce the number of routes that they advertise to routers in the network, to exclude routes that are not relevant to a particular device. The filtering to reduce the number of routes is based on the colors of TLOCs on each device. For example, a route to a public TLOC is not relevant to a router that only has private TLOCs. Advertising fewer routes helps to avoid reaching the send path limit for routers in the network.
Cisco Catalyst SD-WAN Bridging	
Layer 2 and Layer 3 Flex Port Support	Cisco SD-WAN Manager provides flex support on Layer 2 switchports on Cisco IOS XE Catalyst SD-WAN devices, allowing flexibility for LAN ports at Layer 2 to be converted to Layer 3 ports. You can configure the flex ports on Layer 2 as Layer 3 ports using feature profiles and CLI add-on profile.

Feature	Description
Cisco Catalyst SD-WAN AppQoE	
UCS-E Series Next Generation Support for Deploying Cisco Catalyst 8000V	With this feature, you can deploy Cisco Catalyst 8000V instances, on supported routers, using the UCS-E series blade server modules. With this feature, the UCS-E1100D-M6 server module is supported.
Cisco Catalyst SD-WAN Commands	
show tech-support sdwan bfd	This feature adds support for displaying BFD information on Cisco IOS XE Catalyst SD-WAN devices.

Table 2: Cisco Catalyst SD-WAN Control Components Release 20.11.1

Feature	Description
Co-Management: Improved Granular Configuration for Resource group features	To enable a user to self-manage specific configuration tasks, you can assign the user permissions to perform specific configuration tasks while excluding other tasks. This feature introduces new permission options for the following configuration groups and feature profiles. • AppQoE under other feature profile • GPS under transport feature profile • Cisco VPN Interface GRE under WAN/LAN profile. • Cisco VPN Interface IPsec under WAN profile. • Cisco Multicast under LAN profile. • UCSE under other feature profile. • IPv4 Tracker and Tracker Group under transport and service feature profiles. • IPv6 DIA Tracker and Tracker Group, under transport feature profile.
SCM Integration Improvements	This feature allows you to access Support Case Manager (SCM) wizard using Cisco SD-WAN Manager. You can create, view, or edit the support cases directly from Cisco vManage without having to go to a different Case Manager portal.
Cisco Catalyst SD-WAN Monitor and Maintain	
Enhancement to On-Demand Troubleshooting	You can view the detailed troubleshooting progress of the flow of traffic from a device.

Feature	Description
View Sites in Global Topology View	You can view all sites or a single site in global topology view for geographical regions worldwide by clicking the inverted-drop-shaped icon on the **Monitor Overview** dashboard.
Cisco Catalyst SD-WAN Getting Started Guide	
CRL-Based Quarantine	This feature enables you to quarantine SD-WAN edge devices based on a certificate revocation list that Cisco SD-WAN Manager obtains from a root certificate authority.

Software and Hardware Behavior Changes in Cisco vManage Release 20.11.x

Table 3: Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.11.1a

Behavior Change	Description
To avoid flapping of tracker and tunnels, a interval duration added between the tunnel status. When tunnel status change continuously within a short period of time, tunnel goes to the flapping state. To prevent tunnels flap, an interval multiplier is configured on the tracker configuration.	Updated the Tracker Parameters section with a note for Multiplier field.
When the Cisco Catalyst SD-WAN sessions with QoS policy reaches the maximum limit, QoS policy will not be applied for the new SD-WAN sessions.	Updated the Overview of Per-Tunnel QoS section with the note on Per-Tunnel QoS scale parameter to configure maximum Cisco Catalyst SD-WAN sessions.
DH groups are used in IKE to establish session keys. As part of security hardening and deprecation of weak ciphers, the option to configure Diffie-Hellman groups (DH) groups 1, 2, and 5 are removed and these are not supported.	Updated the Configure IPsec Tunnel Parameters section with the note on supported DH groups.
SNMP v3 users with SHA-256 and AES-256 authentication must use 1161 as special port.	Updated the note on using special port in Configure SNMPv3 section.
In a multi-tenant scenario, when configuring controller certificate authorization (**Administration** > **Settings** > **Controller Certificate Authorization**), if you configure certificate signing request (CSR) properties manually, some new conditions apply.	Updated the note in the Authorize a Controller Certificate for an Enterprise Root Certificate section.
In Cisco vManage, access the **Cisco Networking Bot** by clicking the **?** icon at the top-right corner of a page and choose **Ask Cisco Networking** from the drop-down list.	You can use Cisco Networking Bot chat to get relevant answers to your questions. A topic in the Cisco IOS XE Catalyst SD-WAN Release Notes 17.11.x covers the details of the CNB.

Behavior Change	Description
In Cisco vManage, while configuring devices, you can switch between the **vManage** and **CLI** modes at a device level.	Notes are added to the Change Configuration Modes topic with steps that describe how to switch between the vManage mode and CLI mode.
Alarms display the hostname as **localhost** during the cluster setup until the hostname is configured in Cisco vManage.	Updated the Configure the Cluster IP Addresssection with a note on default hostname.
New commands are added to display data policy that a Cisco SD-WAN Controller has pushed to the devices and the tags downloaded from the Cisco SD-WAN Controller.	Following new commands are added: • show sdwan from-vsmart policy • show sdwan from-vsmart tag-instances is added.
Cisco vManage Release 20.11.1 does not support the QoS map feature in the transport profile and the service profile.	Before upgrading to Cisco vManage Release 20.11.1, ensure that you delete the QoS map feature from the transport profile or the service profile if you have already configured it. For the procedure to delete the QoS map, see: • QoS Map in the Transport and Management profile. • QoS Map in the Service profile.
New debug and show commands are added to Cisco Cloud OnRamp for SaaS.	35 new debug and show commands are added to Debug and Show Commands section.

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.

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	20.11.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.	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	20.11.x
			Check disk space* • If the disk space is more than 25 GB, Direct Upgrade • If the disk space is less than 25 GB, Stepwise upgrade through 20.1 • If you are upgrading to 20.6, the additional 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	20.11.x
			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	20.11.x
20.1.x	Not Supported	Not Supported	Direct Upgrade For cluster upgrade procedure: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade through 20.3.x 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.	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	20.11.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 `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 `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 `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 `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 `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 `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 `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	20.11.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 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.	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	20.11.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 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	20.11.x
20.6.x	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										
	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	20.11.x
										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 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	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 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

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	20.11.x
										Cisco SD-WAN Manager Release 20.1.1 and later.	Cisco SD-WAN Manager Release 20.1.1 and later.
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 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.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	20.11.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 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.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	20.11.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 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.
20.10.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade

To check the free disk space using CLI,

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

Cluster upgrade must be performed using CLI

- 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 20.11.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 20.11.1.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.11.1.2

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 20.11.1.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Releases 20.11.1.1

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

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.11.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.11.1

Identifier	Headline
CSCwd95581	VRRP timer in Cisco SD-WAN Manager UI - default 100ms
CSCwc61501	OIB: Cisco SD-WAN Manager Restriction of special chars in Remote server pwd addition field needs to be removed
CSCwe32116	Cisco SD-WAN Manager : DSPFarm template error "Duplicate value:mediaresourcegroupname"
CSCwd79186	Cisco SD-WAN Manager generating corrupted TAR file for config-db backup on 20.3.4.0.5
CSCwe34379	Cisco SD-WAN Manager access failed when accessing Cisco SD-WAN Manager using DNS record
CSCwd90841	Cisco SD-WAN Manager Dashboard: WAN Edge Health Widget shows invalid / unconfigured edges in poor health status

Identifier	Headline
CSCwd16027	Unable to generate report from Cisco SD-WAN Manager for SLP Offline mode - Error occurred while generating report
CSCwb58176	SSO/ciscotacro/rw User Session invalidated when browser switches between Cisco SD-WAN Manager nodes in cluster
CSCwe14017	20.6.5 Cisco vBond and Cisco vSmart upgrade fail via Cisco SD-WAN Manager UI
CSCwe59364	Monitor -> Logs -> Events page is displaying only one entry partially
CSCwd62984	OMPD crashed in Cisco vSmart on ISE config removal
CSCwd96644	Not able to edit the PIM interface for Cisco IOS XE SD-WAN devices feature template.
CSCwd94301	MTT correlation engine not generating OMP Alarms from OMP Event received from Cisco vSmart
CSCwe26568	Cisco SD-WAN Manager multitenancy do not report licenses after provider credentials are changed.
CSCwd45547	Cannot set VPN ID value as 'Device Specific' on 'TACACS group' AAA feature template
CSCwe53807	[20.11.0-169] SIT setup: DR - config-db crash in the secondary cluster
CSCwd65132	Cisco vEdge Cloud Cloud Init on OpenStack : Parent Interfaces are assigned fixed IPs from Openstack
CSCwd37102	Support two Separate EIGRP Key Chains for 2 EIGRP Processes
CSCwe40153	Devices that are upgraded are marked as skipped when 1 device fails upgrade in upgrade task
CSCwc04446	Default route is not installed in the routing table of VPN 0 if the VNIC is changed in OpenStack
CSCwa77149	API call /dataservice/statistics/dpi/aggregation returns error 500
CSCwe31950	Cisco SD-WAN Manager HTTP/HTTPS Settings break DR process even after adding the Cluster IPs in the non-proxy list
CSCwd96434	Cisco SD-WAN Manager "Renew Device CSR" task cannot be opened under completed tasks
CSCwe11554	Unused System IP Pool subnet cannot be deleted
CSCwd55134	Exception handling in Cisco SD-WAN Manager code does not return details about the exception we are hitting
CSCwd60889	CPU average values reported to Cisco SD-WAN Manager are incorrect
CSCwd26472	Cisco SD-WAN Manager : DSPFarm template not accepting multiple variable fields for "CUCM Media Resource Name"
CSCwb43140	Cisco SD-WAN Manager in cluster of 6 rebooting with Software initiated - sysmgr got signal 11
CSCwe31884	RBAC Configurational Group bug on 20.9.1 Software Version
CSCwd90919	Controller server logging priority config does not take effect
CSCwd31522	20.10 :Edit of single VPC fails to do mapping as required
CSCwd23197	Default umask value needs to be changed for security reason for upgrade usease

Identifier	Headline
CSCwd73212	ciscotacro and ciscotacrw login on vmanage is not creating an entry in audit log
CSCwd69360	SIG feature template will not retain tunnel destination modified variable names Cisco SD-WAN Manager 20.6.4
CSCwc61498	vnf-ha-net reused causing HA formation to FAIL
CSCwd01820	Disaster recovery syslogs are set as information priority instead of correct priority
CSCwd46415	Cisco SD-WAN Manager deactivates active central policy using API
CSCwd52998	Nutella migration should not be allowed if there is a config-group associated with the router
CSCwe04530	Application-server keep restarting after upgrading on 20.10.1 from 20.9.2
CSCwd07860	Cisco SD-WAN Manager is redirecting to wrong IDP when same domains are used in a certain order.
CSCwd64838	[SIT]: Wrong SIG credentials were sent to device from CLI template.=> 20.10/17.10
CSCwd40824	API call /dataservice/statistics/dpi/aggregation returns error 500
CSCwd28593	Control connection flap of assigned vSmart after shutting down other assigned Cisco vSmart
CSCwd61771	Remove SDAVC cloud connector settings in tenant view
CSCwe26011	Cisco SD-WAN Manager is not generating alarm notifications to be sent to Webhooks server.
CSCwd37096	Enabled usage but prepaid consumption - Product instance "UDI_PID:Cisco_vManage
CSCvz86879	statistics/on-demand/queue POST returns 500 error even though object was created correctly
CSCwe75147	20.12: DCA connection over proxy timing out on Cisco SD-WAN Manager
CSCwd35047	Failed to ping gateway while configuring SharedLOM with console , te1 interface. until router reload
CSCvz62234	Cisco Catalyst SD-WAN Manager Unauthorized Configuration Rollback Vulnerability
CSCwd46383	Cisco SD-WAN Software Denial of Service Vulnerability

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.11.1

Identifier	Headline
CSCwe63470	Audit does not bring all tunnels up in specific scenario
CSCwe23381	Deploy fails when device has brown field BGP configuration from feature/device template.
CSCwe37804	Tenant device list is not pushed to the new Cisco SD-WAN Manager node so no control connection to device
CSCwe63222	Certificate output is not getting changed on renew when Cloud Certificate Authorization is Automated
CSCwe17455	template push failure
CSCwe51543	Stats db in boot-loop after upgrading from 20.10 to 20.11, UI inaccessible
CSCwe88453	Cisco SD-WAN Manager not including net mask for BGP for a /32

Identifier	Headline
CSCwe51379	Config group and feature profiles do not have view option for operator user
CSCwe91258	Wireless Template cannot be attached to a C1113-8PLTELAWZ device
CSCwe76283	Cloud Gateway Attachment is not shown for dedicated mode after tag is unmapped
CSCwe68861	Unable to delete device from MTT vmanage
CSCwd90586	Cisco SD-WAN Manager scrollbar is executing several API calls that slow down the performance
CSCwe53624	Cisco SD-WAN Manager: cURL may flag error on ca cert file "Error in the time fields of certificate"
CSCwe54749	Error 'Multiple tenants are active simultaneously' seen randomly on vmanage UI

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 vManage 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.

Cisco SD-WAN Manager GUI Changes

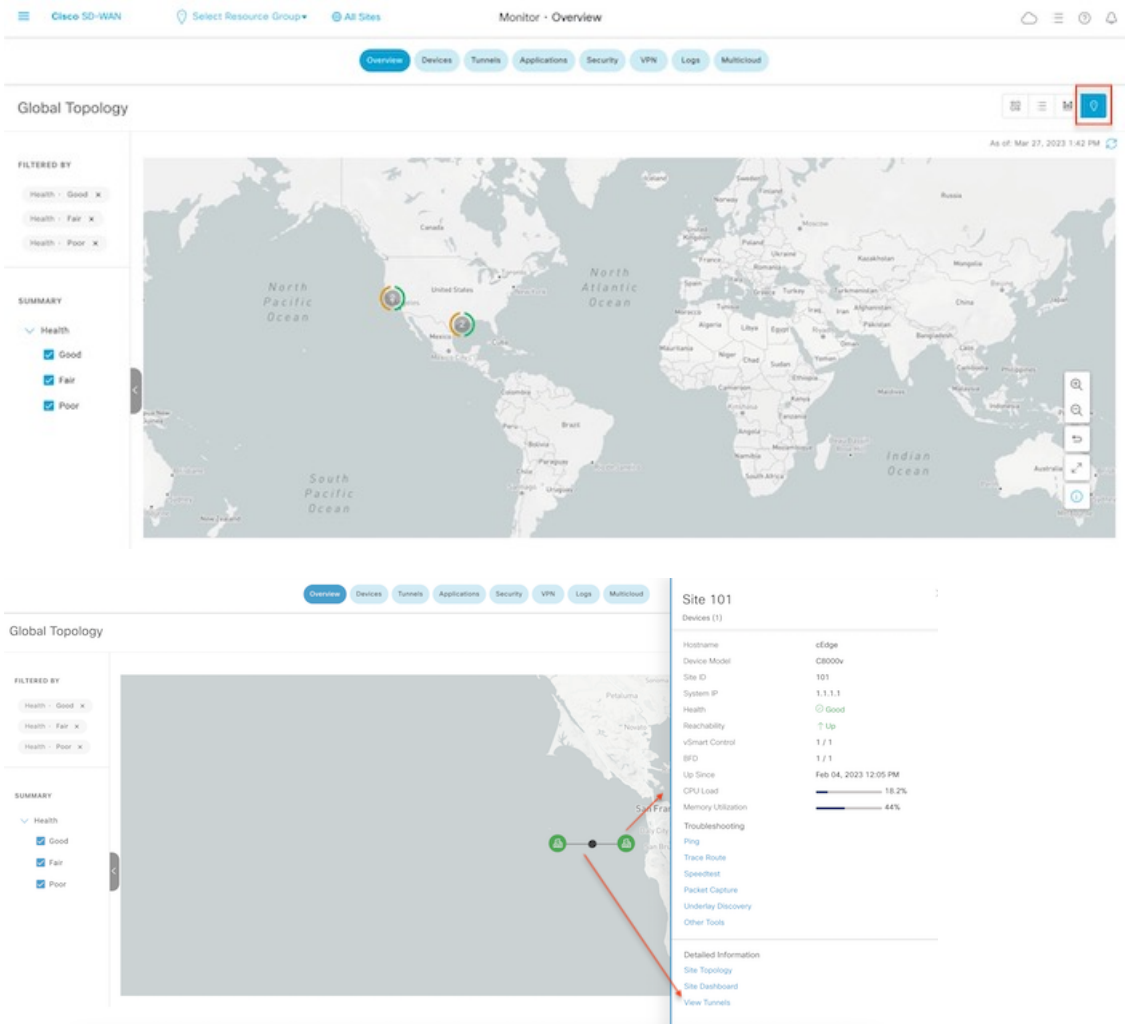
This section presents a comparative summary of the significant GUI changes between Cisco vManage 20.10.x and Cisco vManage Release 20.11.1.

Monitor Overview Page

In Cisco vManage Release 20.11.1, the following GUI changes have been made to the **Monitor** > **Overview** page. For more information about the **Monitor** > **Overview** page, see Cisco SD-WAN Manager Monitor Overview.

- The global topology view has been added to the page.

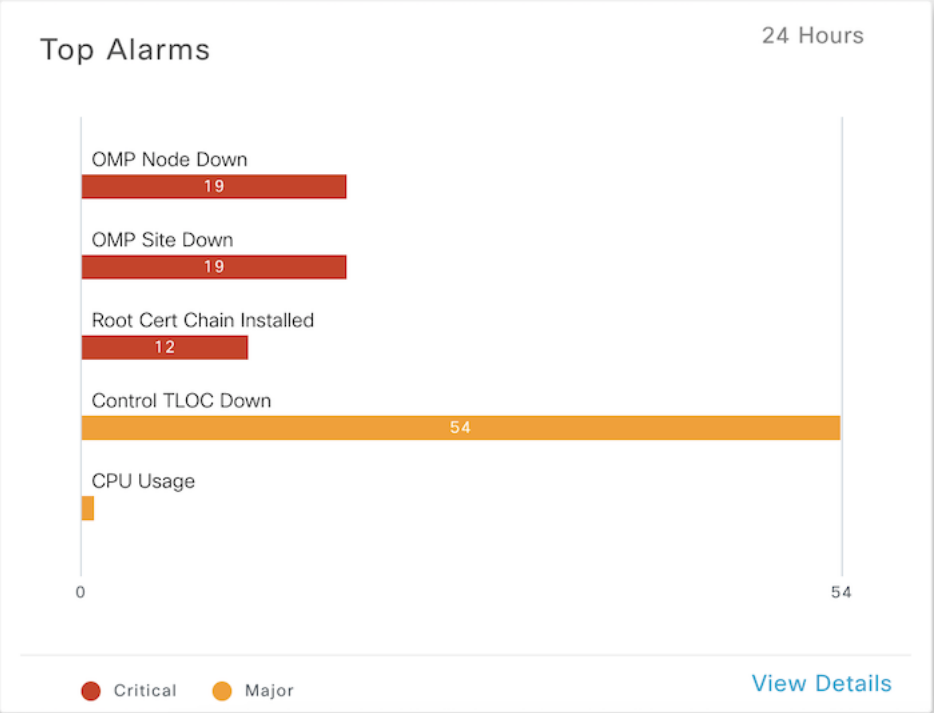
Figure 1: Global Topology View of the Monitor Overview Page in Cisco SD-WAN Manager 20.11.1



- New dashlets, **WAN Edge Management** in all sites and **Top Alarms** in single site have been added.

Figure 2: New Dashlet WAN Edge Management in the Monitor Overview Page in Cisco SD-WAN Manager 20.11.1

Figure 3: New Dashlet Top Alarms in the Single Site Monitor Overview Page in Cisco SD-WAN Manager 20.11.1



On-Demand Troubleshooting

In Cisco vManage Release 20.11.1, on-demand troubleshooting progress has been added to the page.

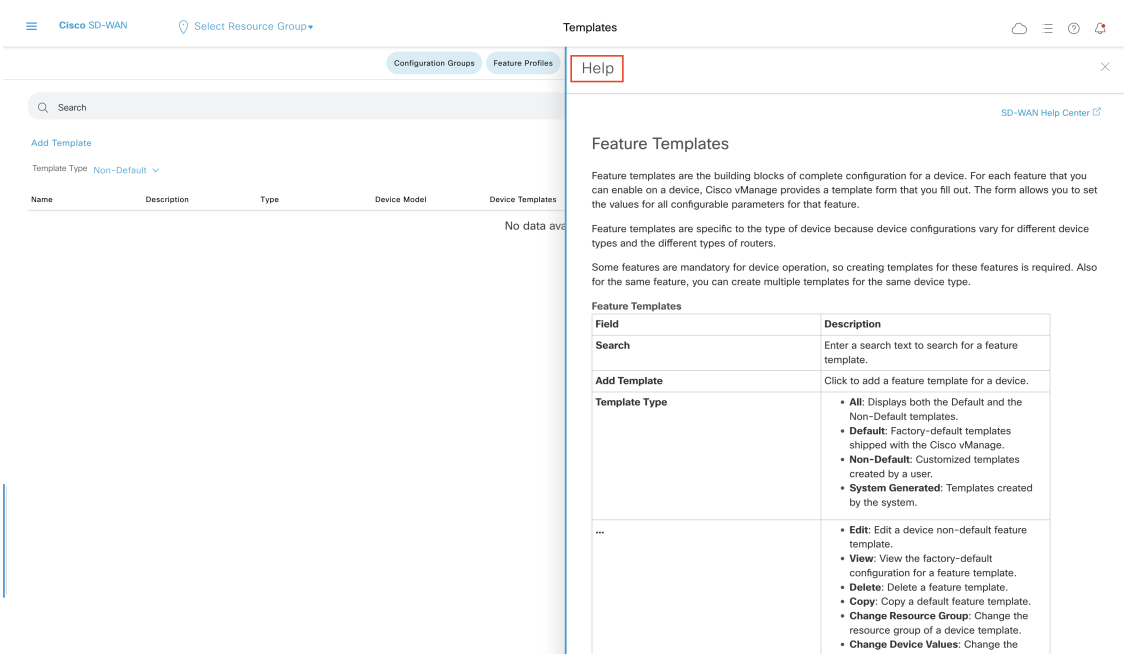
Figure 4: Enhance On-Demand Troubleshooting Processing Time in Cisco SD-WAN Manager 20.11.1

In-product Help

In a single-tenant deployment, access help content for Cisco SD-WAN Manager UI pages by clicking the **Help** icon at the top-right corner of a page. The help content is displayed in a slide-in pane in the same browser window.

Starting from Cisco SD-WAN Manager Release 20.12.x, In-product help is available for a majority of the Cisco SD-WAN Manager UI pages.

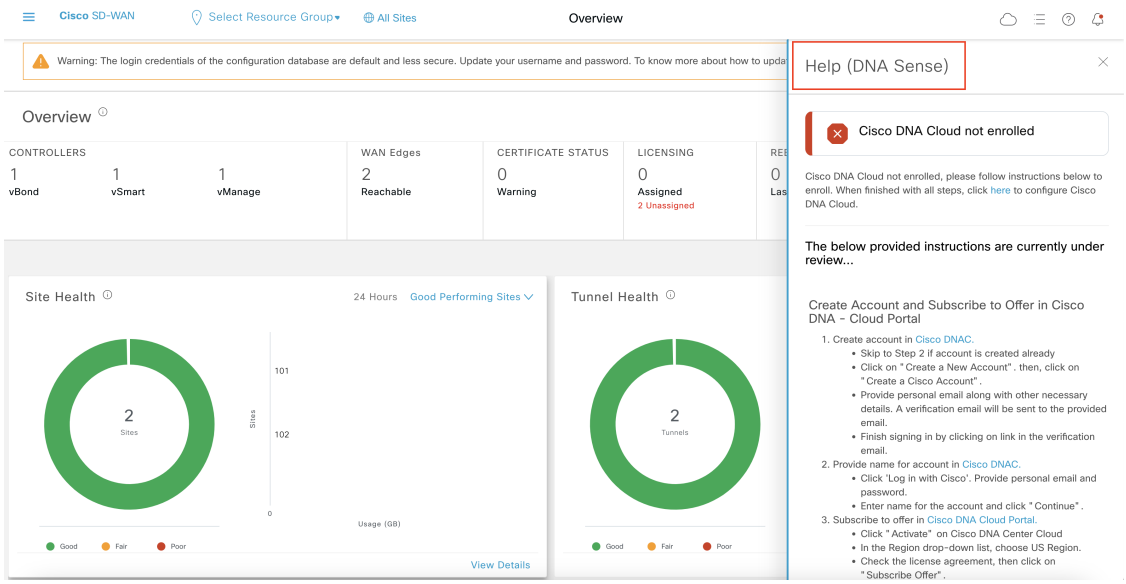
Figure 5: Help Content in a Slide-in Pane



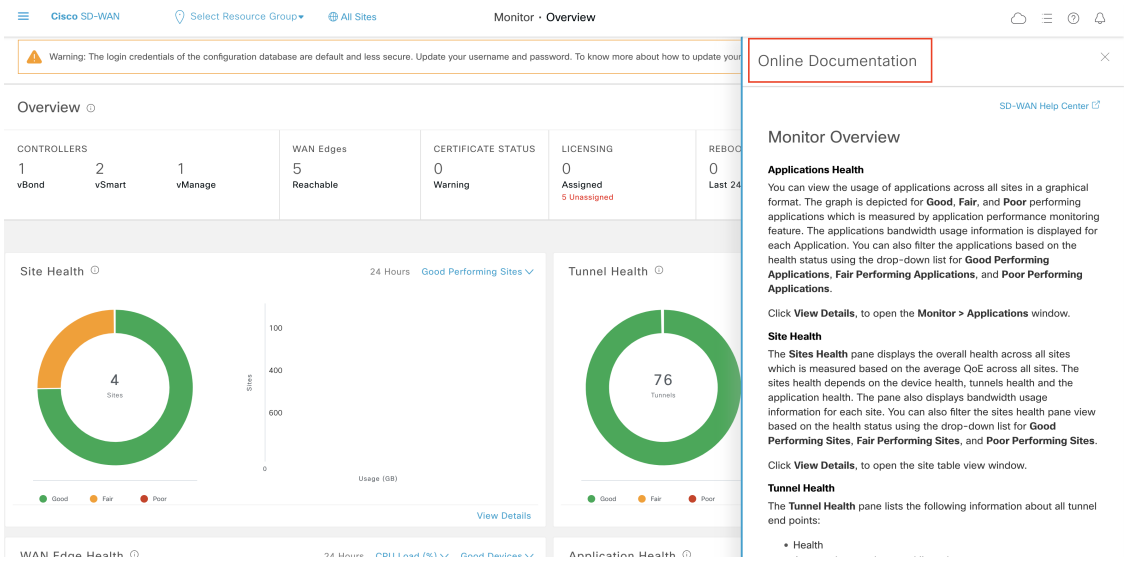
Cisco DNA Sense

Access help content for Cisco SD-WAN Manager UI pages using Cisco DNA Sense by clicking the **?** icon at the top-right corner and choose **Help (DNA Sense)** from the drop-down list.

Cisco DNA Sense is not enabled by default for all the users. You should enroll and configure your Cisco SD-WAN Manager using the instructions provided in the **Help (DNA Sense)** pane. The help content from Cisco DNA Sense is displayed across all major Cisco SD-WAN Manager pages once you enroll.



If your Cisco SD-WAN Manager is already enrolled to Cisco DNA Sense, choose **Online Documentation** from the **?** drop-down.



Ask Cisco Networking Bot

To access the **Cisco Networking Bot** click the **Help(?)** icon and choose **Ask Cisco Networking** from the drop-down list.

You can use Cisco Networking Bot chat to get relevant answers to your questions.

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)