Release Notes for Cisco Catalyst SD-WAN Control Components Release 20.12.x

First Published: 2023-08-22

Last Modified: 2024-07-30

Read Me First

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

Related References

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations
- Cisco Catalyst SD-WAN Device Compatibility

User Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17
- User Documentation for Cisco SD-WAN Release 20

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.

- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

Release Notes for Cisco SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.12.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 Catalyst SD-WAN Control Components, Release 20.12.x, which provides Cisco Catalyst SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager as applicable to Cisco Catalyst SD-WAN.

Related Releases

For release information about Cisco IOS XE Catalyst SD-WAN devices, refer to Release Notes for Cisco IOS XE Catalyst SD-WAN device, Cisco IOS XE Release 17.12.x.

What's New for Cisco Catalyst SD-WAN Control Components Release 20.12.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 17.12.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started Guide	
Support for Certificates Without the Organizational Unit Field	Enterprise certificates that you install on devices do not require the Organizational Unit (OU) field to be defined. Earlier, this field was used as part of the authentication of a device. However, if a signed certificate includes the OU field, the field must match the organization name configured on the device.

Feature	Description
Cisco Catalyst SD-WAN Systems and Interfaces	
Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN Mode	This feature enables you to configure the following Cisco Catalyst SD-WAN Remote Access features for a device in SSL-VPN mode, using Cisco SD-WAN Manager: — Private IP Pool — Authentication — AAA Policy
Configuration Groups and Feature Profiles (Phase IV)	The following new features are introduced to the feature profiles: — In the System Profile: Flexible Port Speed. — In the Transport Profile: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, T1/E1 Controller — Subfeatures for transport VPN: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, T1/E1 Serial, DSL PPPoE, DSL PPPoA, DSL IPoE, Ethernet PPPoE — In the Service Profile: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, EIGRP Routing, Object Tracker, Object Tracker Group — Subfeatures for service VPN: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, EIGRP Routing, Multilink Controller, Object Tracker, Object Tracker Group — The **Route leak to Global VPN** option is added to the **Route Leak** parameter in the service VPN.
Support for Dual Device Site Configuration	This feature supports dual devices site configuration using configuration groups, for redundancy.
Enhancements to User-Defined Device Tagging	Device tagging has the following new functionalities: — When you add devices to a configuration group using rules, you can choose **Match All** or **Match Any**. — You can use **Starts With** and **Ends With** operator conditions when you add devices to a configuration group using rules. — In addition, the button formerly called **Add New Tag** is now **Create New Tag**.
VFR (Virtual Fragmentation Reassembly) and Underlay Fragmentation	The VFR mechanism reassembles fragmented packets in Cisco Catalyst SD-WAN networks. The packets are fragmented for better transportion and are fragmented while they are travelling through a VFR enabled Cisco IOS XE Catalyst SD-WAN device. Underlay fragmentation fragments packets in the underlying layer of a network. Underlay fragmentation is introduced to easily transport larger packets that exceed the (MTU).
Enhanced Cisco Catalyst SD-WAN Manager Dashboard for Multitenancy	This feature is enhanced to support consistent user experience in tenant and service providers dashboard. The Cisco Catalyst SD-WAN Manager dashboard provides visibility into the available resources on shared devices.

Feature	Description
RADIUS/TACAS Support for Multitenancy	This feature enables support for Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS) authentication in a multitenant deployment on WAN edge devices.
Enhanced Multitenant Tier Definition to include NAT Limits	This feature is enhanced to support NAT to enforce per tenant maximum limit on the translations. From this release **Tier** is called **Resource Profile** in Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN Routing Configuration Guide	
Transport Gateways	A transport gateway operates as the hub in a hub-and-spoke routing topology. It offers the advantage of achieving this topology without requiring complex routing policy configuration. The following are some uses of a transport gateway: • Providing connectivity to routers in disjoint underlay networks • Serving as a gateway (hub) for all traffic in one discrete network to reach another discrete network, such as directing all local network traffic to a cloud gateway
Hub-and-Spoke Configuration	Hub-and-spoke configuration simplifies the process of configuring a hub-and-spoke topology, making complex centralized control policy unnecessary. Instead, the configuration requires only a few simple configurations: a single command each on (a) the Cisco SD-WAN Controllers serving a network, (b) a router that serves as a hub, and (c) the routers that operate as spokes.
Symmetric Routing	You can use affinity groups, affinity group preference, and translation of RIB metrics to ensure symmetric routing of traffic flows across devices in a network. Symmetric routing accommodates various network topologies, including Multi-Region Fabric. To support symmetric routing beyond the overlay network, transport gateways can translate RIB metrics to control plane protocols such as BGP and OSPF. This extends the path preference configuration to routers outside of the overlay network, such as routers in a data center LAN.
Cisco Catalyst SD-WAN Policies	
WAN Insight Policy Automation	With this feature, you can apply the recommendations that are available on vAnalytics to Cisco SD-WAN Manager AAR policy and view the applied recommendations on Cisco SD-WAN Manager.
Flow Telemetry Enhancement When Using Loopbacks as TLOCs.	When you configure a loopback interface as an ingress or egress transport interface, this feature enables you to collect loopback interface reports in FNF records and is supported for IPv4 and IPv6. A show command is enhanced on the device to display the binding relationship between the loopback and physical interfaces.
Lawful Intercept 2.0 Enhancements	This feature lets you configure intercepts in the Cisco Catalyst SD-WAN multitenancy mode, and also provides support for Cisco Catalyst SD-WAN Manager clusters.

Feature	Description
Enhancements to Flexible NetFlow for vAnalytics	This feature introduces logging enhancements to Cisco Flexible NetFlow for Cisco SD-WAN Analytics. The output of the **show flow record** command has been enhanced for IPv4 and IPv6 flow records.
Enhanced Application-Aware Routing	Without enhanced application-aware routing enabled, Cisco IOS XE Catalyst SD-WAN device require several minutes to switch traffic from one network path to another to meet SLA requirements when the loss, latency, and jitter exceed specific threshold values. Enabling enhanced application-aware routing speeds the detection of tunnel performance issues. This enables Cisco IOS XE Catalyst SD-WAN devices to redirect traffic away from tunnels that do not meet SLA requirements.
Cisco Catalyst SD-WAN Security	
Snort Engine Version Upgrade	This feature adds support for Snort engine version 3, which is an upgrade from version 2.
IPv6 GRE or IPsec Tunnels Between Cisco Catalyst SD-WAN and Third-Party Devices	This feature allows you to configure an IPv6 GRE or IPSEC tunnel from a Cisco IOS XE Catalyst SD-WAN device device to a third-party device over a service VPN.
Enabling MACsec using Cisco SD-WAN Manager	This feature adds support for enabling MACsec using Cisco SD-WAN Manager for Cisco Catalyst SD-WAN devices on the service side. With MACsec enabled using Cisco SD-WAN Manager, communication between devices in the service VPN is protected, thus enhancing security for the service VPN.
OMP Prefixes for IP-SGT Binding	The OMP routes are typically present in the IOS RIB. The OMP routes aren't present in the IOS FIB containing entries that map destination IP addresses to next-hop IP addresses. The IOS FIB operates independently of the control plane, receiving the forwarding instructions from a centralized Cisco SD-WAN Controller instead of consuming the OMP routes from the IOS RIB. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the OMP prefixes get added to the IOS FIB which improves IP-SGT binding.
Cisco Catalyst SD-WAN Cloud OnRamp	
AWS Cloud WAN Integration	AWS Cloud WAN is a managed wide-area network (WAN) service. This feature enables you to easily connect and route remote sites, regions and cloud applications over the AWS global network. You can build and operate the wide-area networks using simple network policies and get a complete view of the global network.
Added an Azure Instance Type	For the Microsoft Azure West Central US and Australia East regions, added the Standard_D16_v5 Azure instance type, which includes 16 CPU cores and 64 GB of memory. You can deploy this type of instance for SKU scale values of 20, 40, 60, and 80.

Feature	Description
Cisco Catalyst 8000V Edge Software Support	You can deploy a Cisco Catalyst 8000v Edge Software as the Interconnect Gateway in the Equinix fabric and connect an Cisco Catalyst SD-WAN branch location to the Interconnect Gateway.
Addition of VPC and VNet Tags to SDCI Connections	You can add or modify additional properties of Virtual Private Cloud (VPC) and Virtual Networks (VNets) tags that are associated with a connection.
Audit Management in Equinix	You can identify the gaps or disconnects between Cisco SD-WAN Manager intent and what is realized in the cloud. The audit management helps in understanding if the interconnect cloud and provider states are in sync with the Cisco SD-WAN Manager state.
Cisco Catalyst SD-WAN Policy Groups	
Policy Groups	This feature provides a simple, reusable, and structured approach for configuring policies in Cisco Catalyst SD-WAN. You can create a policy group, that is, a logical grouping of policies that is applied to one or more sites or a single device at the site in the network. To deploy the policy group to devices, the devices must be managed by a configuration group in Cisco Catalyst SD-WAN. You can configure policies based on features that are required, recommended, or uniquely used, and then combine them to complete a policy configuration.
Security Policy Using Policy Groups	This feature provides a simple, reusable, and structured approach for configuring security policies in Cisco Catalyst SD-WAN. You can create a security policy, that is, a logical grouping of policies that is applied to one or more sites or a single device at the site in the network. To deploy the policy group to devices, the devices must be managed by a configuration group in Cisco Catalyst SD-WAN. You can configure policies based on features that are required, recommended, or uniquely used, and then combine them to complete a policy configuration.
Topology	This feature allows you to provision a **Mesh** or a **Hub and Spoke** topology policy which is applied to Cisco Catalyst SD-WAN Controllers. This allows exchange of data traffic between two or more Cisco IOS XE Catalyst SD-WAN devices.
Cisco Catalyst SD-WAN Monitor and Maintain	
Heatmap View for Alarms	In the heatmap view, a grid of colored bars displays the alarms as **Critical**, **Major**, or **Medium & Minor**. You can hover over a bar or click it to display additional details at a selected time interval. The intensity of a color indicates the frequency of alarms in a severity level.
Heatmap View for Events	In the heatmap view, a grid of colored bars displays the events as **Critical**, **Major**, or **Minor**. You can hover over a bar or click it to display additional details at a selected time interval. The intensity of a color indicates the frequency of events in a severity level.
Enhancements to Audit Logging	This feature introduces enhanced audit logging to monitor unauthorized activity. To view these audit logs, from the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Audit Log**.

Feature	Description
Enhancements to Network-Wide Path Insight	This feature provides enhancements to the Network-Wide Path Insight feature to include support for multiple VPNs for traces, the ability to generate synthetic traffic for traces, options for grouping trace information, support for auto-on tasks, new information on insight displays, and expanded insight summaries.
Cisco Catalyst SD-WAN NAT	
Support for multiple WAN Links for NAT66 DIA	You can configure NAT66 to use multiple WAN Links to direct local IPv6 traffic to exit directly to the internet.
Cisco Catalyst SD-WAN Remote Access	
Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN mode Using Cisco SD-WAN Manager	This feature enables you to configure Cisco Catalyst SD-WAN Remote Access for a device in SSL-VPN mode, using Cisco SD-WAN Manager.
User Login Options	
Configure Inactivity Lockout	You can to configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.
Configure Unsuccessful Login Attempts Lockout	You can configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a designated period.
Configure Duo Multifactor Authentication	You can configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to Cisco SD-WAN Manager.
Cisco IOS XE SD-WAN Qualified Command Reference	
vDaemon Logging Commands	The following troubleshooting commands are added: • **debug vdaemon** • **debug platform software sdwan vdaemon** • **set platform software trace vdaemon** • **show sdwan control connections**
lockout-policy Command	This command allows you to lock out users who have made a designated number of consecutive unsuccessful login attempts within a designated period, or who have not logged in for a designated number of days
multi-factor-auth duo command	This command allows you to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in.

Table 2: Cisco Catalyst SD-WAN Control Components Release 20.12.1

Feature	Description
Cisco Catalyst SD-WAN Security	
Security Dashboard Enhancements	This feature enhances the security dashboard to provide greater flexibility while troubleshooting security threats down to a device level in Cisco Catalyst SD-WAN.
Cisco Catalyst SD-WAN Analytics	
Easy Onboarding of Cisco SD-WAN Analytics into Cisco Catalyst SD-WAN Manager	This feature enables you to easily onboard Cisco SD-WAN Analytics into Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN Monitor and Maintain	
Global Network View with Network-Wide Path Insight Integration	Network-Wide Path Insight is now integrated with the global network view. This feature also introduces enhancements to the geomap view by providing real-time monitoring of the health of each site. **Global Topology View** is now called as **Global Network View** in Cisco SD-WAN Manager.

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.
- The following enhancements are available in Cisco SD-WAN Manager while configuring multiple IdPs for single sign-on:
  - You can set one IdP as a default IDP.
  - While configuring a domain name, you have the option to enter a domain name with a wildcard (*), which will make that domain the default domain. If a default domain is configured, you can log in to a domain with just the user ID (john) without requiring you to enter an user ID in email address format (john@mystore.com).
- From Cisco Catalyst SD-WAN Manager Release 20.12.x, Cisco SD-WAN Manager accepts only HTTP POST requests for logging out from Cisco SD-WAN Manager. It does not support the use of the GET method for this function.

  Refer to developer.cisco.com for more details.

Cisco SD-WAN Manager Upgrade Paths

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

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

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

Starting Cisco SD-WAN Manager Version	Destination Version						
	20.6.x	**20.7.x**	**20.8.x**	**20.9.x**	**20.10.x**	**20.11.x**	**20.12.x**
20.6.x	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade from 20.9.5.2 and later releases.	Step upgrade from 20.6.1, 20.6.2, and 20.6.3 either to 20.6.4 or 20.9.5.2 and later releases. or Direct upgrade from 20.6.4 or 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.6.1, 20.6.2, and 20.6.3 either to 20.6.4 or 20.9.5.2 and later releases. or Direct upgrade from 20.6.4 or 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.6.1, 20.6.2, and 20.6.3 either to 20.6.4 or 20.9.5.2 and later releases. or Direct upgrade from 20.6.4 or 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version						
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x
20.7.x	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade from 20.9.5.2 and later releases	Step upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version						
	20.6.x	**20.7.x**	**20.8.x**	**20.9.x**	**20.10.x**	**20.11.x**	**20.12.x**
20.8.x	Not Supported	Not Supported	Not Supported	Direct Upgrade from 20.9.5.2 and later releases.	Step upgrade from 20.9.5.2 and later releases For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.9.5.2 and later releases For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.9.5.2 and later releases For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version						
	20.6.x	**20.7.x**	**20.8.x**	**20.9.x**	**20.10.x**	**20.11.x**	**20.12.x**
20.9.x	Not Supported	Not Supported	Not Supported	Not Supported	Direct upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	

Starting Cisco SD-WAN Manager Version	Destination Version						
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x
							Direct Upgrade from 20.9.5.2 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** • We recommend the data base size in the disk is less than or equa to 5GB. Use the `request nms configuration-c diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisc SD-WAN Manager Release 20.1.1 and later. • If your Cisco Catalyst SD-WAN Manager is running Cisc

Starting Cisco SD-WAN Manager Version	Destination Version						
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x
							vManage Release 20.9.x and you are looking to upgrade to Cisco Catalyst SD-WAN Manager Release 20.12.x, we recommend you use the CLI mode of configuration for cluster upgrades. If Cisco Catalyst SD-WAN Manager UI is used for upgrading a cluster, the cluster's nms process fails when the new partition is activated. Continue to use the Cisco Catalyst SD-WAN Manager UI and CLI for standalone Cisco SD-WAN Manager upgrades.
20.10.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade

Starting Cisco SD-WAN Manager Version	Destination Version						
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x
20.11.x	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

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.

Resolved and Open Bugs for Cisco SD-WAN Controllers 20.12.x

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.4

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.4

Identifier	Headline
CSCwi71976	UI changed needed for CSCwi56821 MT License Settings exposed at Tenant Level.
CSCwj39272	Site health shows yellow when circuit of last resort configured.
CSCwi56821	MT license settings exposed at Tenant Level.
CSCwf98797	Summary page of nfv CG workflows shows value of "color" for the field that is labeled as "Type"
CSCwh89309	NFVIS 4.12.1 : Transport interfaces down after a FDR on nfvis
CSCwi91313	1131x device shows as HSEC compatible NO in vManage &gt;&gt; license management.
CSCwh55434	Elastic search server CPU high due to JVM JIT deoptimization issue on getMonthOfYear()
CSCwf90168	False error "Subject serial num mistmatch" come up on ZTP server syslog.

Identifier	Headline
CSCwj39215	Selecting 3-dots next to BGP feature does not save Edge01 or Edge02.
CSCwc04678	The data-policy-commit-failure notification promote to Alarm.
CSCwj34301	Cisco SD-WAN Manager custom group user is not able to run speed test with 'Forbidden Request: roleNotAllowed'
CSCwj23827	Cisco SD-WAN Manager DR : Replication stuck and not even attempting to create further exports
CSCwi72623	Change partition task stuck, during Cisco SD-WAN Manager upgrade activation from 20.12 to 20.14
CSCwi62044	SD-AVC container mount point change in Cisco SD-WAN Manager results in lost custom apps post-upgrade.
CSCwi10675	Devices with pull mode stats collection stops working after upgrade to Cisco Catalyst SD-WAN Manager Release 20.13.x latest.
CSCwi72111	/dataservice/device/action/install/devices/{deviceType} not working in apidocs page
CSCwi57614	Cisco SD-WAN Manager: Enterprise Feature Certificate Authorization domain name issue
CSCwj17284	The communication between Cisco SD-WAN Manager cluster gets break due to routes overlapping with Eth4 interface.
CSCwj29915	Preferred color group not available in traffic policy.
CSCwj39594	6-Node cluster DR Replication not working in certain scenario .
CSCwi43016	Need pop-up to display warning banner on 20.9 and 20.12 stating "SHA/AES-128 deprecation"
CSCwi45974	Unable to save the TACACS Server configuration when using Configuration Groups.
CSCwj04353	DCA is not sending device list data for MT Tenants.
CSCwj24314	[20.9.4] High memory utilization for wildfly.
CSCwj77415	Expanded Communities not populating in UI when creating Match sequence on pre-existing policies.
CSCwi21976	Cisco SD-WAN Manager API: User with only Interface read-only access can see the connected user list.
CSCwi85554	Cisco SD-WAN Manager cannot deploy a configuration group on a Cisco IOS XE Catalyst SD-WAN deviceadded by a tag rule
CSCwi75078	The banner issue on Cisco IOS XE Catalyst SD-WAN device from feature template Cisco SD-WAN Manager 20.9.4.1
CSCwi64908	The /dataservice/statistics/approute/fec/aggregation API takes much longer after upgrade

Identifier	Headline
CSCwi99563	Unable to Edit Object Tracker on Static NAT Entries when there are a lot of entries.
CSCwi56971	Cisco SD-WAN Manager 20.12.2 / Search tool of Select smart/virtual accounts to fetch/sync licenses is not working
CSCwi95474	6 + 6 DR cluster elects replication leader which has no config-db and fails to connect to neo4j
CSCwi81830	20.12.3: unable to login to Cisco SD-WAN Manager after enabling proxy- AAAMgr auth req failed with exception.
CSCwk07246	Need to address collection thread issue.
CSCwi74398	DCA Rest: MT: If some tenant uploads fail, further tennats may be skipped.
CSCwj09144	Cisco SD-WAN Manager || Intermittent request time out while trying to access administration user groups
CSCwi49242	After upgrading Cisco SD-WAN Manager to 20.12.2, local/AAA users won't be able to login after 10-15 mns reboot
CSCwh36350	"/logout" method should be updated to POST in API Doc for 20.12 Cisco SD-WAN Manager
CSCwh24335	Manipulate driver of Neo4j and ES to use static logger instead of new logger (Cisco SD-WAN Manager Slowness 20.6)
CSCwi60266	Cisco IOS XE Catalyst SD-WAN device with enterprise certificates not forming control connections with controllers after upgrade
CSCwk05068	No space left on device error seen on Cisco SD-WAN Controller.
CSCwj82987	Cisco-Hosted Catalyst Manager - Custom apps not recovered after upgrade to 20.10+
CSCwi72014	CDCS Tenant - SSH tool not working
CSCwj75749	Edit of basic parcel fails with "Required But Missing Attributes for transportGateway.value"

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.4

Identifier	Headline
CSCwk09812	Cisco SD-WAN Manager upgrade to version 20.12.3 with 32vCPU on-prem High CPU alarms
CSCwk20837	Route sent count is wrong in omp summary when Control Policy for TE is used.
CSCwh02871	Multiple alarms APIs RBAC is not working as expected.
CSCwb56080	Fail to deploy config group when AAA accounting "start stop" is set to False.
CSCwk14925	Cisco SD-WAN Validator running 20.6.5.2 experiencing kernel panic

Identifier	Headline
CSCwk55344	Cisco SD-WAN Manager 20.12.3 Group of Interest not working properly when creating "Application List"
CSCwk37657	The devices brought up with PNP when pre deployed to a config group do not receive the full configuration
CSCwk37838	Copy of configuration group with Dual device type is creating as single router type.
CSCwk61283	Traffic class option not available when creating a traffic policy list.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.3.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.3.1

Identifier	Headline
CSCwi49242	After upgrading Cisco SD-WAN Manager to 20.12.2, local/AAA users won't be able to login after 10-15 mns reboot.
CSCwj82987	Cisco-Hosted Catalyst Manager - Custom apps not recovered after upgrade to 20.10+
CSCwj39594	6-Node cluster DR Replication not working in certain scenario.
CSCwi95474	6 + 6 DR cluster elects replication leader which has no config-db and fails to connect to neo4j.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.3.1

Identifier	Headline
CSCwm70614	Stats data not visible after upgrading to 20.12.3.1 MTT setup.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.3

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.3

Identifier	Headline
CSCwi29893	Unable to configure tracker group when object tracker is configured as route.
CSCwf68955	Cisco SD-WAN Manager Log Poisoning bypass
CSCwf68959	Cisco SD-WAN Manager Audit Log CSV payload injection
CSCwf75967	Cisco SD-WAN Manager Malicious File Upload vulnerability
CSCwi33594	The DCA folder is piling UP with small files which is exhausting the space.
CSCwi65635	Cisco SD-WAN Manager is creating config with 3 x "router eigrp" configs which is not supported.

Identifier	Headline
CSCwh81907	APN profile password was found in plain text when Cellular profile template was configured.
CSCwd94839	Cisco SD-WAN Manager GUI becomes unavailable due to authentication errors against configuration-db.
CSCwi27589	Cloud on ramp for multicloud deploy fails with error : Azure Error: RequestDisallowedByPolicy
CSCwh46931	Cisco SD-Branch: Failed to create network design: Failed to update one or more device profiles
CSCwe80348	Cluster creation may fail due to store ID mismatch in neo4j.
CSCwh16901	The HSEC license installation from the workflow does not complete.
CSCwi83788	/var/log/vconfd is filled with repeated messages pointing to Python cb_get_object error.
CSCwi00334	LAN intf name in dual router config group workflow is getting modified after CG creation.
CSCwh83203	MT: Centralized policy push with overlapping sites is returing success but Cisco SD-WAN Controller rejects it.
CSCwi03952	Cisco SD-WAN Manager Template push failure | Failed to update configuration - CLI generation failed.
CSCwh04968	Control Session PPS increase and reset during the upgrade for Cisco vEdge device.
CSCwh18874	Replication takes 4+ hours to inject the 100MB of data on standby cluster-no make primary to switch
CSCwi80950	The Auto-Correct audit feature is deleting the cloudgateways in Multicloud after connectivity issues.
CSCwh02439	Cisco SD-WAN Manager - Unable to add devices to Cloud on Ramp for SaaS due to timeout while loading device list.
CSCwh87880	The usage of policy group for security configuration random push error.
CSCwi24780	Alarm:Analytics is enabled but relevant license is not present.
CSCwj05119	Cannot scroll up/down the drop down check list properly.
CSCwh85507	Fix error message on Cisco SD-WAN Manager when deploying configuration group have policy group attached.
CSCwh41461	Any new created Policy-Config will effact the update history of other Policy-Groups.
CSCwh80773	During periodic audit of Azure CoR if there is an AuthorizationFailed, Cisco SD-WAN Manager will remove CoR.

Identifier	Headline
CSCwh38837	API call for dataservice/management/elasticsearch/index/size/estimate is failing.
CSCwf07155	"Set CSR Properties" for Controllers Cert Auth setting on Cisco SD-WAN Manager GUI is not getting disabled
CSCwi23113	Dual device site workflow is not generating correct key for vrrp IP address variable.
CSCwi62833	The SNMPv3 is not listening on IPv6 interface after Cisco SD-WAN Manager reload.
CSCwf95165	The vdaemon file is incomplete when generating a Cisco SD-WAN Manager admin-tech using GUI.
CSCwh29957	CLI Add-On Template's Config Diff shows wrong configuration.
CSCwh45608	20.9: IP Subnet Pool is not discovered when creating Azure CGW using existing vHUB.
CSCwi59963	The DCA process is continuously restarting after upgrade to 20.9.3.2
CSCwh73298	After upgrading the Cisco SD-WAN Manager from 20.6.x to 20.9.3 ES, the standby Cisco SD-WAN Manager reports down status.
CSCwh81740	API call (dataservice/device/tloc) retrieve an additional color which is not present on the device.
CSCwh46024	Cisco SD-WAN Manager is not starting new traces due to high scaled full mesh network.
CSCwi43409	20.9/20.12: enforce character length validation for user, usergroup, password via confD
CSCwh28301	Cisco SD-WAN Manager GUI becomes very slow when a large template.
CSCwf40110	The option to add Switchport in the Configuration Group Templates is not available.
CSCwi01270	Cannot overwrite a FW security policy with a CLI add-on template, configuration is not seen on device
CSCwh11161	Device template fails on 20.6.5.2 due to SNMP community string.
CSCwf66968	Solution: "Failed to create/initialize database : vmanagedb" and node1 UI is not accessible.
CSCwh73776	20.13: Missing control-connection CLI Generation in CG.
CSCwh12619	"Routing DNA Essentials: Tier 0: 05M" is not available to choose in Cisco SD-WAN Manager GUI
CSCwh62321	Cisco SD-WAN Manager 20.12.1 / admintech upload tool is failing.
CSCwh93441	Cisco SD-WAN Manager: Unable to login SSH including ciscotacro/ciscotacrw.
CSCwi21156	SDCI-Azure connection creation failsAzure Error:PublicIpWithBasicSkuNotAllowedOnExpressRouteGateways
CSCwh66310	Intermittently the SSO user with tenantadmin privilege only getting basic access.

Identifier	Headline
CSCwi30235	Issue with accessing Cisco SD-WAN Manager 20.6.6 GUI using upper-case letter on TACACS username
CSCwi04213	On-prem: New cloud services OTP doesn't get updated via API if OTP is already present in db.
CSCwh62306	Cisco SD-WAN Manager DR fails in the event that a vBond is unreachable.
CSCwi05515	DR Replication taking 2 hours for ~100 MB Size
CSCwh18738	Licenses unapplied from License Management in Cisco SD-WAN Manager after DR failover/failback.
CSCwi07172	The ssh and ntp are enabled by default in config. groups

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.3

Identifier	Headline
CSCwi72623	Change partition task stuck, during Cisco SD-WAN Manager upgrade activation from 20.12 to 20.14.
CSCwi53711	Cisco Catalyst SD-WAN Controller upgrade from 20.9.4.1-li to 20.12.2-li fails because of CDB boot error.
CSCwf34015	Unable to push template due to "no ip cef distributed"
CSCwb56080	Fail to deploy config group when AAA accounting "start stop" is set to False.
CSCwi16436	Lan Tracker: Configuration are not saved with correct ip address.
CSCwj09144	Cisco SD-WAN Manager || Intermittent request time out while trying to access administration user groups.
CSCwj12763	The ip name-server command not pushed to Cisco IOS XE Catalyst SD-WAN device.
CSCwj12589	Cisco IOS XE Catalyst SD-WAN device- dns-server addresses in dhcp config are pushed in wrong order.
CSCwh02871	Multiple alarms APIs RBAC is not working as expected.
CSCwj09324	Failed to deploy device with Policy Group. Connection event can be set for inspect action only.
CSCwi95474	6 + 6 DR cluster elects replication leader which has no config-db and fails to connect to neo4j
CSCwi99163	The statistics-database stops importing data with reason : Bulk insertion failur
CSCwj34301	Cisco SD-WAN Manager custom group user is not able to run speed test with 'Forbidden Request: roleNotAllowed'

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.2

Identifier	Headline
CSCwh05956	20.12.2: Alarms corresponding to events are not showing up on Cisco SD-WAN Manager for few devices with DR configuration.
CSCwf75967	Cisco SD-WAN Manager Malicious File Upload vulnerability
CSCwh25000	Cannot overwrite a FW security policy with a CLI add on template.
CSCwh11913	SD-WAN workflows ST and MT VNF primary image path is missing additional file path specified in virtual image page.
CSCwf90207	Edit of variables in additional settings is not working.
CSCwf81695	Unable to add more than 30 VPN Interface SVI.
CSCwh84962	Cisco Catalyst SD-WAN Controller withdraws TLOC RIB out after going into GR.
CSCwf98777	Cisco Catalyst SD-WAN Controller policy is not sending the updated TLOC information.
CSCwh22127	Software initiated reboot due to OMPD crash (segmentation fault).
CSCwh32413	Fixed typo in diagnostics log filename.
CSCwd85558	The app-server java process is not initiating in 6 node 20.6 cluster .
CSCwh01870	Template push failed post Cisco SD-WAN Manager upgrade from 20.4 to 20.9 "udp udp-src-dst-port-list source range"
CSCwh24243	Suppress OMP advertisement of stale versioned TLOCs on Cisco Catalyst SD-WAN Controller
CSCwh11629	Template shows out of sync due to control flap caused by hardware Cisco Catalyst SD-WAN Edge device enterprise cert install.
CSCwf50089	Template push fails when ZBFW policy has sequences matching UDP ports 500/4500 in Cisco SD-WAN Manager 20.9
CSCwh26907	Cisco SD-WAN Manager GUI SaaS probe endpoint type URL is not allowing to use "-" character as value.
CSCwf93420	SD-WAN workflows/20.12.2: LAN OSPFv3 IPv4/IPv6: sub-feature parcel failed to be saved.
CSCwh88227	Application list with duplicate name entries in "Group of Interest".
CSCwf95317	Devices are not receiving the preference via the policy in a Multi-Tenant environment.
CSCwh30799	SD-WAN workflows missing nocloud property in payload when checked in Cisco SD-WAN Manager NFV config group UI.

Identifier	Headline
CSCwh48782	TACACS netadmin users are not able to acess vshell on 20.12.
CSCwf83985	20.12:AWS-With Pure IPV6 overlay, vbond vpn 0 ge0/0 interface if-oper-status down after power off/on.
CSCwe90415	Massive update for feature template fails.
CSCwh24574	Application SLA traffic policy with base action allow without any match field is ignored.
CSCwf09036	Cisco SD-WAN Manager configures incorrect IKEv2 lifetime for IPSec tunnels.
CSCvt47226	Routes missing on a Cisco Catalyst SD-WAN Edge devices in a graceful-restart scenario.
CSCwf85996	In Multi-Tenant Cisco SD-WAN Manager, Equinix ICGW is stuck in LIVE state, and not changing to ACTIVE state.
CSCwh06082	Unable to create Azure CGW using NVA created from Azure Portal.
CSCwf86315	Error unlocking device configuration mode to CLI mode.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.2

Identifier	Headline
CSCwh62321	Cisco SD-WAN Manager_20.12.1 / admintech upload tool is failing.
CSCwh02871	Multiple alarms APIs RBAC is not working as expected.
CSCwf34015	Unable to push template due to "no ip cef distributed".
CSCwh69041	20.13:SDCI connection using Multicloud TGW marked as success / traffic fails.
CSCwb56080	Failed to deploy configuartion group when AAA accounting "start stop" is set to False.
CSCwh87880	The usage of policy group for security configuration has random push error.
CSCwh62306	Cisco SD-WAN Manager DR fails in the event that a Cisco Catalyst SD-WAN Validator is unreachable.
CSCwh28301	Cisco SD-WAN Manager GUI becomes very slow when a large template with 1000+ variables is uploaded.
CSCwh97370	The NAT DIA interface &lt; name&gt; overload egress-interface &lt; interface&gt; is not pushed to Cisco IOS XE Catalyst SD-WAN device.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.1

Identifier	Headline
CSCwe95606	Double GR_Additional log enablement defect
CSCwf68955	Cisco SD-WAN Manager Log Poisoning bypass
CSCwf68959	Cisco SD-WAN Manager Audit Log CSV payload injection
CSCwe66540	Cisco Catalyst SD-WAN : Decommissioning or deleting device did not release the license.
CSCwe95368	- AAR Default SLA values changing by the system
CSCwf68886	Cisco SD-WAN Manager deletes the custom folder whenever editing the IPS settings
CSCwf48674	Cisco IOS XE Catalyst SD-WAN device unified security policy template fails to enable geo database
CSCwf98724	20.11/12 ST/MT: updating app server logo via nms command is not working
CSCwf21372	Cisco SD-WAN Manager does not recognize the resource group for resource group admin login via TACACS
CSCwf63511	OSPFv3 - "Advertise" command not appearing on OSPFv3 for IPV4 address-family
CSCwe85177	Scroll up or down under feature template box change the values.
CSCwe83858	Unable to update DHCP Tunnel interface template if template was cloned from factory default template
CSCwe42158	Cisco SD-WAN Manager GUI : Incorrect Average Values for Latency/Jitter/Loss percentage for Edge Routers
CSCwe57259	Template pushed with wrong APN settings, Cisco SD-WAN Manager shows wrong APN config even after rollbacked.
CSCwe91258	Wireless Template cannot be attached to a C1113-8PLTELAWZ device
CSCwe88453	Cisco SD-WAN Manager not including net mask for BGP for a /32
CSCwf10147	Topology API showing only data links on Cisco Edge devices
CSCwe76283	Cloud Gateway Attachment is not shown for dedicated mode after tag is unmapped
CSCwf63112	Unable to edit the user group's created under Administration &gt; Manage Users.
CSCwf03555	Cisco SD-WAN Manager unable to parse certain timezones and is triggering certificate installation process
CSCwf45552	Cisco Catalyst SD-WAN CoR for SaaS - Enable O365 Application Error
CSCwf51992	Need to hide/remove "key" field in TACACS server configuration in AAA template

Identifier	Headline
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"
CSCwe31281	20.9 Autotunnel Ipsec tracker:Tracker does not come up at all on vedge
CSCwd54278	aaamgr process restarts unexpectedly
CSCwf67622	Cisco SD-WAN Manager is loading continuously when a new user access is created with Network Hierarchy.
CSCwf63504	OSPFv3 - "distance" command not showing under address-family ipv4
CSCwe87281	Cisco SD-WAN Manager pushing DH group (14,15,16) for SIG template for IKEv2 (unsupported by Umbrella)
CSCwf49674	Cisco SD-WAN Manager is modifying load_balance .json leading to the edges to be disconnected.
CSCwe63222	Certificate output is not getting changed on renew when Cloud Certificate Authorization is Automated
CSCwf28362	Cisco SD-WAN Manager is not generating alarm notifications to be sent to Webhooks server.
CSCwf34096	168 Cisco vEdge 5000 device inbuilt certificate expiring on 12th Nov 2023
CSCwd46383	Cisco SD-WAN Software Denial of Service Vulnerability

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.12.1

Identifier	Headline
CSCwf82106	20.10 20.11- Localhost can't be modified to IP in Cluster management Page : GRPC error CO for ZK
CSCwh02871	Multiple alarms APIs RBAC is not working as expected
CSCwh16392	20.12-Tacacs server configuration broken for cloud-init config
CSCwh06082	Unable to create Azure CGW using NVA created from Azure Portal
CSCwh24574	Application SLA Traffic Policy with Base Action Allow without any match field is ignored
CSCwf98976	Cannot save application priority & SLA profile if intf value from drop down list is used first time
CSCwh18738	Licenses unapplied from License Management in Cisco SD-WAN Manager after DR failover/failback

Identifier	Headline
CSCwf85996	In Multi-Tenant Cisco SD-WAN Manager, Equinix ICGW is stuck in LIVE state, not changing to ACTIVE state
CSCwh24857	Cisco SD-WAN Manager UI should show the error when Upper case letter present in " User Group Name"
CSCwh24921	17.12 OGREF: Add Cisco SD-WAN Manager restriction for OGREF toggle
CSCwh24577	IPv6 Neighbor doesn't establish with default Application SLA Traffic Policy Simple workflow

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 Catalyst SD-WAN Manager API

For information on Cisco SD-WAN Manager Release 20.12.x APIs, see Cisco SD-WAN Manager API.

Cisco SD-WAN Manager GUI Changes

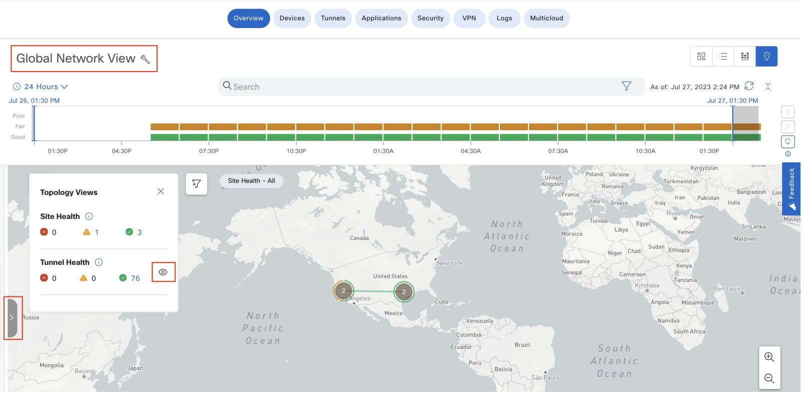
This section presents a comparative summary of the significant GUI changes between Cisco vManage Release 20.11.1 and Cisco Catalyst SD-WAN Manager Release 20.12.1.

Monitor Overview Page

Cisco Catalyst SD-WAN Manager Release 20.12.1 includes the following GUI changes to the **Monitor** > **Overview** page. For more information about the **Monitor** > **Overview** page, see Cisco SD-WAN Manager Monitor Overview.

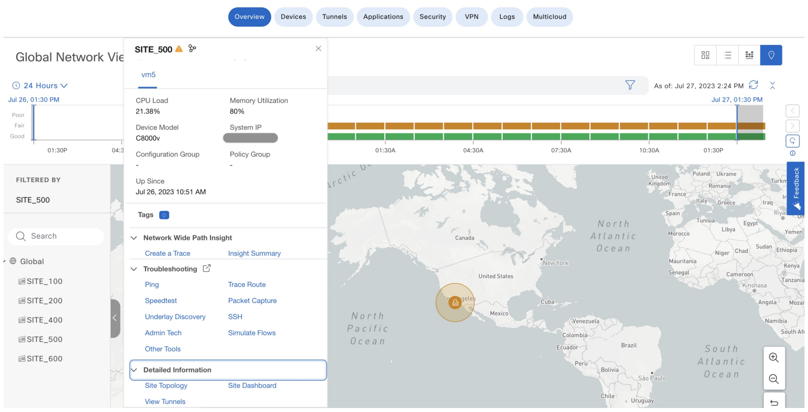
- The **Global Topology** view is called as **Global Network View** in Cisco SD-WAN Manager.

Figure 1: Global Network View in Monitor - Overview Page



Click the eye icon to view the tunnel connection with aggregated tunnel health between the sites. Click the arrow on the left to open the network hierarchy menu.

Figure 2: Device Details for the Selected Site in Global Network View



CPU Load: 21.38%

Memory Utilization: 80%

Device Model: C8000v

System IP: [redacted]

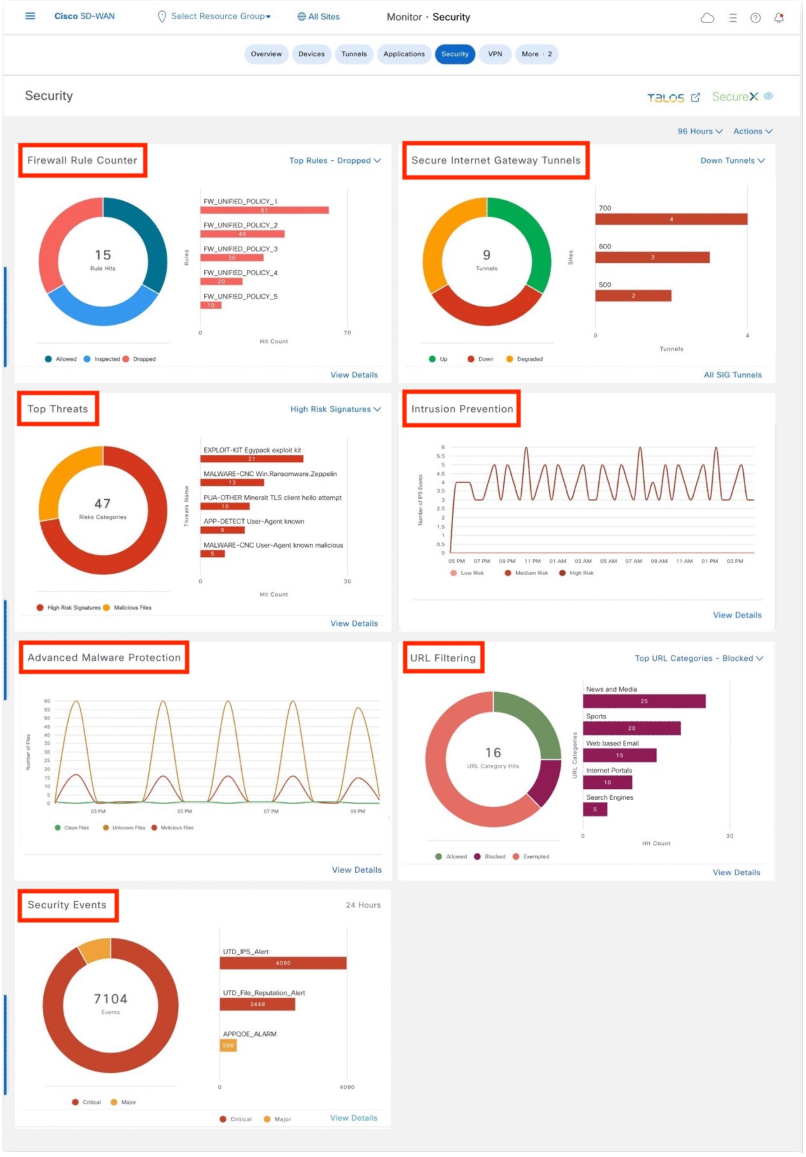
Configuration Group: -

Policy Group: -

Up Since: Jul 26, 2023 10:51 AM

- Cisco Catalyst SD-WAN Manager's security dashboard is enhanced to provide greater flexibility in troubleshooting security threats.

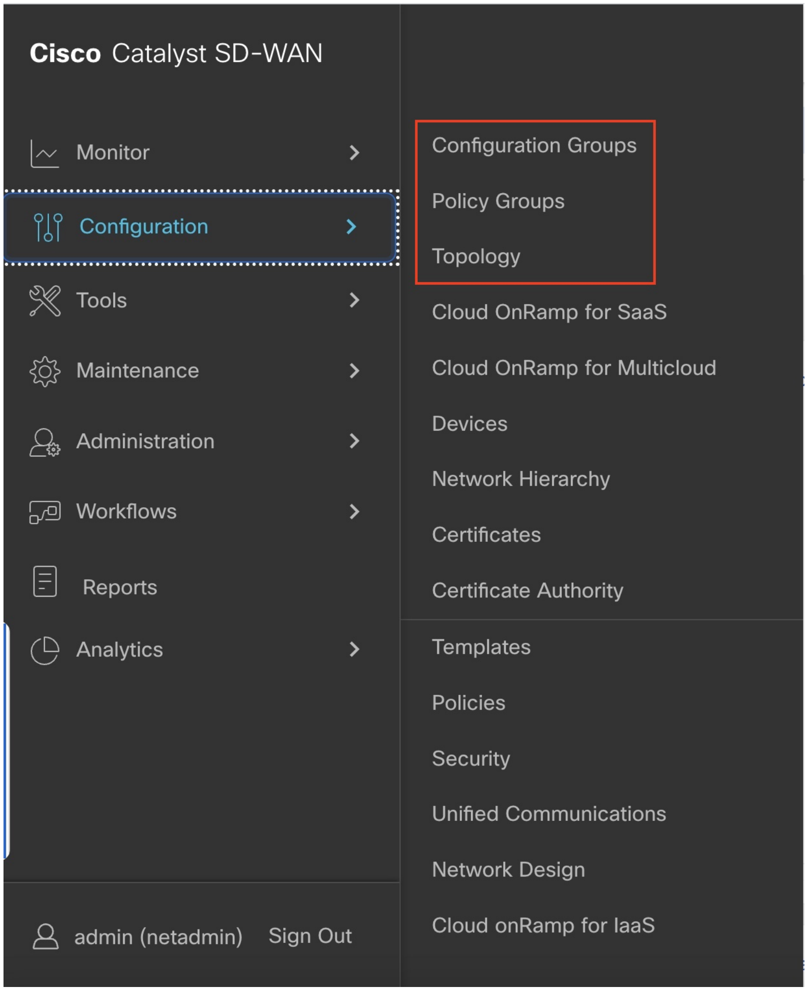
Figure 3: Enhancements to the Security Dashboard Through Modified Dashlets in the Monitor - Security Page



Configuration Page

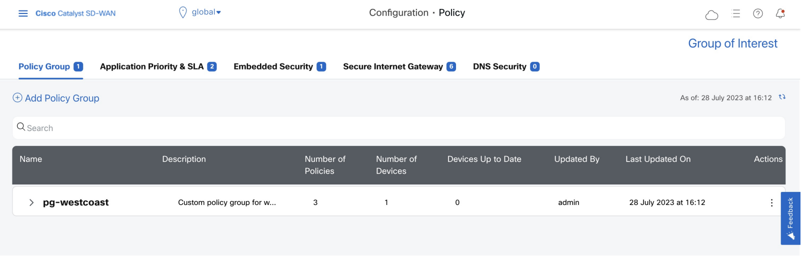
New submenus are added to the **Configuration** menu in Cisco Catalyst SD-WAN Manager menu.

Figure 4: New Submenus in the Configuration Menu



New menus are available in the **Configuration** > **Policy Groups** page to configure policy groups and security policies.

Figure 5: Policy Page for Configuring Policy Groups and Security Policies



As of: 28 July 2023 at 16:12

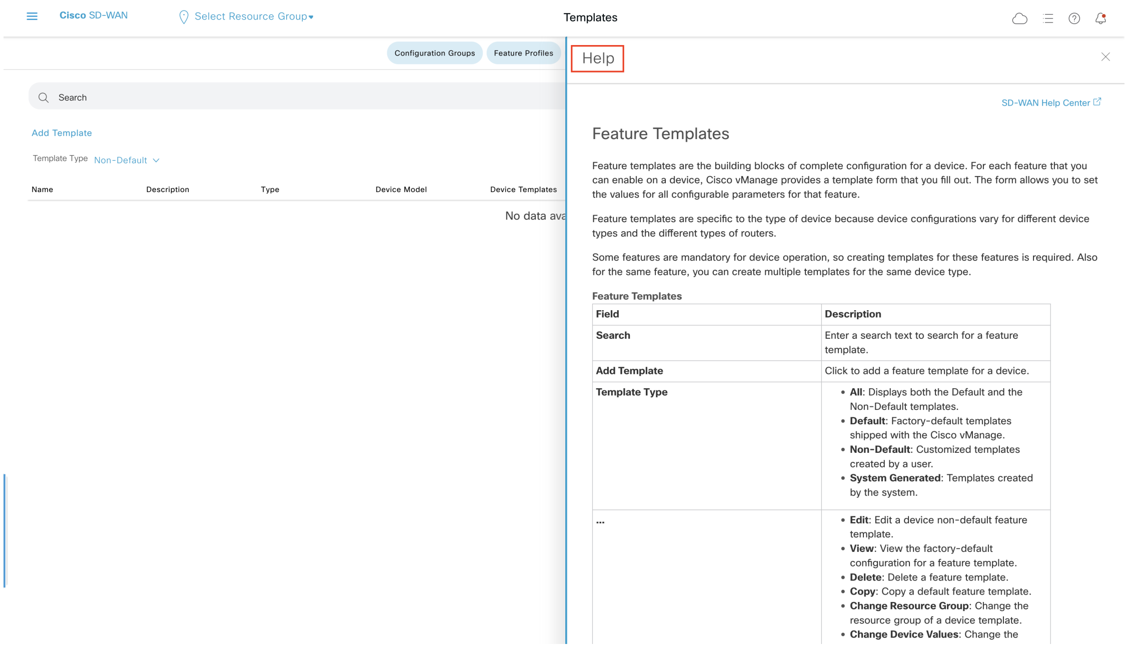
Name	Description	Number of Policies	Number of Devices	Devices Up to Date	Updated By	Last Updated On	Actions
pg-westcoast	Custom policy group for w...	3	1	0	admin	28 July 2023 at 16:12	⋮

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 6: Help Content in a Slide-in Pane



Feature Templates

Feature templates are the building blocks of complete configuration for a device. For each feature that you can enable on a device, Cisco vManage provides a template form that you fill out. The form allows you to set the values for all configurable parameters for that feature.

Feature templates are specific to the type of device because device configurations vary for different device types and the different types of routers.

Some features are mandatory for device operation, so creating templates for these features is required. Also for the same feature, you can create multiple templates for the same device type.

Feature Templates

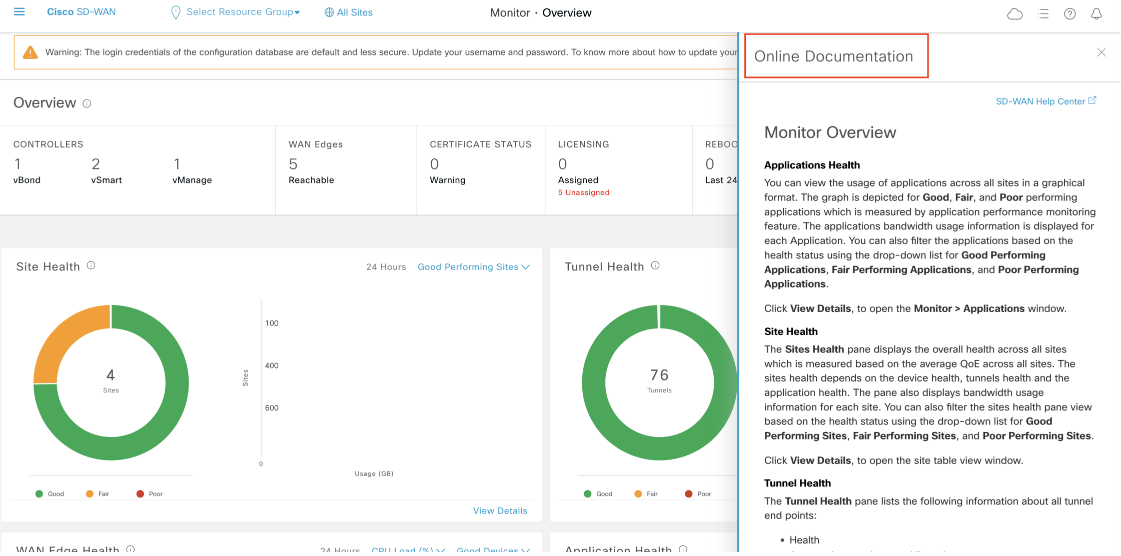
Field	Description
Search	Enter a search text to search for a feature template.
Add Template	Click to add a feature template for a device.
Template Type	• **All**: Displays both the Default and the Non-Default templates. • **Default**: Factory-default templates shipped with the Cisco vManage. • **Non-Default**: Customized templates created by a user. • **System Generated**: Templates created by the system.
...	• **Edit**: Edit a device non-default feature template. • **View**: View the factory-default configuration for a feature template. • **Delete**: Delete a feature template. • **Copy**: Copy a default feature template. • **Change Resource Group**: Change the resource group of a device template. • **Change Device Values**: Change the

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 **Online Documentation** 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 **Online Documentation** 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.



Warning: The login credentials of the configuration database are default and less secure. Update your username and password. To know more about how to update your

Monitor Overview

Applications Health

You can view the usage of applications across all sites in a graphical format. The graph is depicted for **Good**, **Fair**, and **Poor** performing applications which is measured by application performance monitoring feature. The applications bandwidth usage information is displayed for each Application. You can also filter the applications based on the health status using the drop-down list for **Good Performing Applications**, **Fair Performing Applications**, and **Poor Performing Applications**.

Click **View Details**, to open the **Monitor > Applications** window.

Site Health

The **Sites Health** pane displays the overall health across all sites which is measured based on the average QoE across all sites. The sites health depends on the device health, tunnels health and the application health. The pane also displays bandwidth usage information for each site. You can also filter the sites health pane view based on the health status using the drop-down list for **Good Performing Sites**, **Fair Performing Sites**, and **Poor Performing Sites**.

Click **View Details**, to open the site table view window.

Tunnel Health

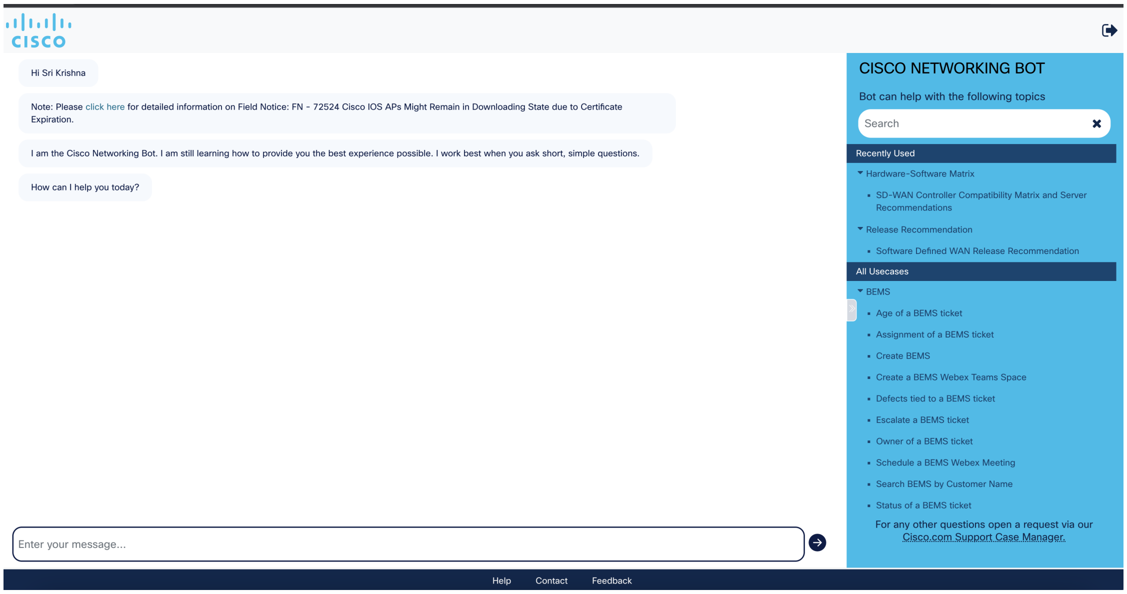
The **Tunnel Health** pane lists the following information about all tunnel end points:

- Health

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.


CISCO
CISCO NETWORKING BOT
Bot can help with the following topics
Search
Recently Used
Hardware-Software Matrix
SD-WAN Controller Compatibility Matrix and Server Recommendations
Release Recommendation
Software Defined WAN Release Recommendation
All Usecases
BEMS
Age of a BEMS ticket
Assignment of a BEMS ticket
Create BEMS
Create a BEMS Webex Teams Space
Defects tied to a BEMS ticket
Escalate a BEMS ticket
Owner of a BEMS ticket
Schedule a BEMS Webex Meeting
Search BEMS by Customer Name
Status of a BEMS ticket
Enter your message...
Help
Contact
Feedback

Hi Sri Krishna

Note: Please click here for detailed information on Field Notice: FN - 72524 Cisco IOS APs Might Remain in Downloading State due to Certificate Expiration.

I am the Cisco Networking Bot. I am still learning how to provide you the best experience possible. I work best when you ask short, simple questions.

How can I help you today?

For any other questions open a request via our Cisco.com Support Case Manager.

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

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.

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.