

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

---

**First Published:** 2023-08-22

**Last Modified:** 2024-03-23

## 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
<b>Cisco Catalyst SD-WAN Getting Started Guide</b>	
<a href="#">Support for Certificates Without the Organizational Unit Field</a>	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
<b>Cisco Catalyst SD-WAN Systems and Interfaces</b>	
<a href="#">Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN Mode</a>	<p>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:</p> <ul style="list-style-type: none"> <li>— Private IP Pool</li> <li>— Authentication</li> <li>— AAA Policy</li> </ul>
<a href="#">Configuration Groups and Feature Profiles (Phase IV)</a>	<p>The following new features are introduced to the feature profiles:</p> <ul style="list-style-type: none"> <li>— In the System Profile: Flexible Port Speed.</li> <li>— In the Transport Profile: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, T1/E1 Controller</li> <li>— Subfeatures for transport VPN: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, T1/E1 Serial, DSL PPPoE, DSL PPPoA, DSL IPoE, Ethernet PPPoE</li> <li>— In the Service Profile: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, EIGRP Routing, Object Tracker, Object Tracker Group</li> <li>— Subfeatures for service VPN: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, EIGRP Routing, Multilink Controller, Object Tracker, Object Tracker Group</li> <li>— The <b>Route leak to Global VPN</b> option is added to the <b>Route Leak</b> parameter in the service VPN.</li> </ul>
<a href="#">Support for Dual Device Site Configuration</a>	<p>This feature supports dual devices site configuration using configuration groups, for redundancy.</p>
<a href="#">Enhancements to User-Defined Device Tagging</a>	<p>Device tagging has the following new functionalities:</p> <ul style="list-style-type: none"> <li>— When you add devices to a configuration group using rules, you can choose <b>Match All</b> or <b>Match Any</b>.</li> <li>— You can use <b>Starts With</b> and <b>Ends With</b> operator conditions when you add devices to a configuration group using rules.</li> <li>— In addition, the button formerly called <b>Add New Tag</b> is now <b>Create New Tag</b>.</li> </ul>
<a href="#">VFR (Virtual Fragmentation Reassembly) and Underlay Fragmentation</a>	<p>The VFR mechanism reassembles fragmented packets in Cisco Catalyst SD-WAN networks. The packets are fragmented for better transportation and are fragmented while they are travelling through a VFR enabled Cisco IOS XE Catalyst SD-WAN device.</p> <p>Underlay fragmentation fragments packets in the underlying layer of a network. Underlay fragmentation is introduced to easily transport larger packets that exceed the (MTU).</p>
<a href="#">Enhanced Cisco Catalyst SD-WAN Manager Dashboard for Multitenancy</a>	<p>This feature is enhanced to support consistent user experience in tenant and service providers dashboard.</p> <p>The Cisco Catalyst SD-WAN Manager dashboard provides visibility into the available resources on shared devices.</p>

Feature	Description
<a href="#">RADIUS/TACAS Support for Multitenancy</a>	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.
<a href="#">Enhanced Multitenant Tier Definition to include NAT Limits</a>	This feature is enhanced to support NAT to enforce per tenant maximum limit on the translations. From this release <b>Tier</b> is called <b>Resource Profile</b> in Cisco SD-WAN Manager.
<b>Cisco Catalyst SD-WAN Routing Configuration Guide</b>	
<a href="#">Transport Gateways</a>	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: <ul style="list-style-type: none"> <li>• Providing connectivity to routers in disjoint underlay networks</li> <li>• 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</li> </ul>
<a href="#">Hub-and-Spoke Configuration</a>	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.
<a href="#">Symmetric Routing</a>	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.
<b>Cisco Catalyst SD-WAN Policies</b>	
<a href="#">WAN Insight Policy Automation</a>	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.
<a href="#">Flow Telemetry Enhancement When Using Loopbacks as TLOCs.</a>	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.
<a href="#">Lawful Intercept 2.0 Enhancements</a>	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
<a href="#">Enhancements to Flexible NetFlow for vAnalytics</a>	<p>This feature introduces logging enhancements to Cisco Flexible NetFlow for Cisco SD-WAN Analytics.</p> <p>The output of the <b>show flow record</b> command has been enhanced for IPv4 and IPv6 flow records.</p>
<a href="#">Enhanced Application-Aware Routing</a>	<p>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.</p> <p>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.</p>
<b>Cisco Catalyst SD-WAN Security</b>	
<a href="#">Snort Engine Version Upgrade</a>	This feature adds support for Snort engine version 3, which is an upgrade from version 2.
<a href="#">IPv6 GRE or IPsec Tunnels Between Cisco Catalyst SD-WAN and Third-Party Devices</a>	This feature allows you to configure an IPv6 GRE or IPSEC tunnel from a Cisco IOS XE Catalyst SD-WAN device to a third-party device over a service VPN.
<a href="#">Enabling MACsec using Cisco SD-WAN Manager</a>	<p>This feature adds support for enabling MACsec using Cisco SD-WAN Manager for Cisco Catalyst SD-WAN devices on the service side.</p> <p>With MACsec enabled using Cisco SD-WAN Manager, communication between devices in the service VPN is protected, thus enhancing security for the service VPN.</p>
<a href="#">OMP Prefixes for IP-SGT Binding</a>	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.
<b>Cisco Catalyst SD-WAN Cloud OnRamp</b>	
<a href="#">AWS Cloud WAN Integration</a>	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.
<a href="#">Added an Azure Instance Type</a>	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
<a href="#">Cisco Catalyst 8000V Edge Software Support</a>	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.
<a href="#">Addition of VPC and VNet Tags to SDCI Connections</a>	You can add or modify additional properties of Virtual Private Cloud (VPC) and Virtual Networks (VNETs) tags that are associated with a connection.
<a href="#">Audit Management in Equinix</a>	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.
<b>Cisco Catalyst SD-WAN Policy Groups</b>	
<a href="#">Policy Groups</a>	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.
<a href="#">Security Policy Using Policy Groups</a>	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.
<a href="#">Topology</a>	This feature allows you to provision a <b>Mesh</b> or a <b>Hub and Spoke</b> 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.
<b>Cisco Catalyst SD-WAN Monitor and Maintain</b>	
<a href="#">Heatmap View for Alarms</a>	In the heatmap view, a grid of colored bars displays the alarms as <b>Critical, Major, or Medium &amp; Minor</b> . 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.
<a href="#">Heatmap View for Events</a>	In the heatmap view, a grid of colored bars displays the events as <b>Critical, Major, or Minor</b> . 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.
<a href="#">Enhancements to Audit Logging</a>	This feature introduces enhanced audit logging to monitor unauthorized activity.  To view these audit logs, from the Cisco SD-WAN Manager menu, choose <b>Monitor &gt; Logs &gt; Audit Log</b> .

Feature	Description
<a href="#">Enhancements to Network-Wide Path Insight</a>	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.
<b>Cisco Catalyst SD-WAN NAT</b>	
<a href="#">Support for multiple WAN Links for NAT66 DIA</a>	You can configure NAT66 to use multiple WAN Links to direct local IPv6 traffic to exit directly to the internet.
<b>Cisco Catalyst SD-WAN Remote Access</b>	
<a href="#">Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN mode Using Cisco SD-WAN Manager</a>	This feature enables you to configure Cisco Catalyst SD-WAN Remote Access for a device in SSL-VPN mode, using Cisco SD-WAN Manager.
<b>User Login Options</b>	
<a href="#">Configure Inactivity Lockout</a>	You can to configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.
<a href="#">Configure Unsuccessful Login Attempts Lockout</a>	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.
<a href="#">Configure Duo Multifactor Authentication</a>	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.
<b>Cisco IOS XE SD-WAN Qualified Command Reference</b>	
<a href="#">vDaemon Logging Commands</a>	The following troubleshooting commands are added: <ul style="list-style-type: none"> <li>• <b>debug vdaemon</b></li> <li>• <b>debug platform software sdwan vdaemon</b></li> <li>• <b>set platform software trace vdaemon</b></li> <li>• <b>show sdwan control connections</b></li> </ul>
<a href="#">lockout-policy Command</a>	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
<a href="#">multi-factor-auth duo command</a>	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
<b>Cisco Catalyst SD-WAN Security</b>	
<a href="#">Security Dashboard Enhancements</a>	This feature enhances the security dashboard to provide greater flexibility while troubleshooting security threats down to a device level in Cisco Catalyst SD-WAN.
<b>Cisco Catalyst SD-WAN Analytics</b>	
<a href="#">Easy Onboarding of Cisco SD-WAN Analytics into Cisco Catalyst SD-WAN Manager</a>	This feature enables you to easily onboard Cisco SD-WAN Analytics into Cisco SD-WAN Manager.
<b>Cisco Catalyst SD-WAN Monitor and Maintain</b>	
<a href="#">Global Network View with Network-Wide Path Insight Integration</a>	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.  <b>Global Topology View</b> is now called as <b>Global Network View</b> 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](https://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	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: <b>request nms configurationdb upgrade</b>	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: <b>request nms configurationdb upgrade</b>	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: <b>request nms configurationdb upgrade</b>

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	Step upgrade from 20.9.x  For cluster upgrade procedure using CLI: <b>request nms configuration upgrade</b>  <b>Note</b>	Step upgrade from 20.9.x  For cluster upgrade procedure using CLI: <b>request nms configuration upgrade</b>  <b>Note</b>	Step upgrade from 20.9.x  For cluster upgrade procedure using CLI: <b>request nms configuration upgrade</b>  <b>Note</b>

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	Step upgrade from 20.9.x  For cluster upgrade procedure using CLI: <b>request nms configuration upgrade</b>	Step upgrade from 20.9.x  For cluster upgrade procedure using CLI: <b>request nms configuration upgrade</b>	Step upgrade from 20.9.x  For cluster upgrade procedure using CLI: <b>request nms configuration upgrade</b>

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  For cluster upgrade procedure using CLI: <b>request nms configuration upgrade</b>	Direct Upgrade  For cluster upgrade procedure using CLI: <b>request nms configuration upgrade</b>	We recommend the data base size in the disk is less than or equal to 5GB. Use the <b>request nms configuration-diagnostic check</b> 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  For cluster upgrade procedure using CLI: <b>request nms configuration upgrade</b>  <b>Note</b>

- We reco the o size disk than to 50 the n nms confi diag com chec data size. appl only upgr devi runn SD- Man Rele 20.1 later
- If yo Cata SD- Man runn vMa Rele 20.9 you

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
20.10.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade
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,

looking  
upgrade  
Cisco  
Catalyst  
SD-WA  
Manage  
Release  
20.12.x,  
recomm  
you use  
CLI mo  
configu  
for clust  
upgrade  
Cisco  
Catalyst  
SD-WA  
Manage  
is used f  
upgradin  
cluster,  
cluster's  
process  
when th  
partition  
activate  
Continu  
use the  
Catalyst  
SD-WA  
Manage  
and CLI  
standalo  
Cisco  
SD-WA  
Manage  
upgrade

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 20.12.3

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

Identifier	Headline
<a href="#">CSCwi29893</a>	Unable to configure tracker group when object tracker is configured as route.
<a href="#">CSCwf68955</a>	Cisco SD-WAN Manager Log Poisoning bypass
<a href="#">CSCwf68959</a>	Cisco SD-WAN Manager Audit Log CSV payload injection
<a href="#">CSCwf75967</a>	Cisco SD-WAN Manager Malicious File Upload vulnerability
<a href="#">CSCwi33594</a>	The DCA folder is piling UP with small files which is exhausting the space.
<a href="#">CSCwi65635</a>	Cisco SD-WAN Manager is creating config with 3 x "router eigrp" configs which is not supported.
<a href="#">CSCwh81907</a>	APN profile password was found in plain text when Cellular profile template was configured.
<a href="#">CSCwd94839</a>	Cisco SD-WAN Manager GUI becomes unavailable due to authentication errors against configuration-db.
<a href="#">CSCwi27589</a>	Cloud on ramp for multicloud deploy fails with error : Azure Error: RequestDisallowedByPolicy
<a href="#">CSCwh46931</a>	Cisco SD-Branch: Failed to create network design: Failed to update one or more device profiles
<a href="#">CSCwe80348</a>	Cluster creation may fail due to store ID mismatch in neo4j.
<a href="#">CSCwh16901</a>	The HSEC license installation from the workflow does not complete.

Identifier	Headline
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 returning 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 effect 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.
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



Identifier	Headline
<a href="#">CSCwh73298</a>	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.
<a href="#">CSCwh81740</a>	API call (dataservice/device/tloc) retrieve an additional color which is not present on the device.
<a href="#">CSCwh46024</a>	Cisco SD-WAN Manager is not starting new traces due to high scaled full mesh network.
<a href="#">CSCwi43409</a>	20.9/20.12: enforce character length validation for user, usergroup, password via confD
<a href="#">CSCwh28301</a>	Cisco SD-WAN Manager GUI becomes very slow when a large template.
<a href="#">CSCwf40110</a>	The option to add Switchport in the Configuration Group Templates is not available.
<a href="#">CSCwi01270</a>	Cannot overwrite a FW security policy with a CLI add-on template, configuration is not seen on device
<a href="#">CSCwh11161</a>	Device template fails on 20.6.5.2 due to SNMP community string.
<a href="#">CSCwf66968</a>	Solution: "Failed to create/initialize database : vmanagedb" and node1 UI is not accessible.
<a href="#">CSCwh73776</a>	20.13: Missing control-connection CLI Generation in CG.
<a href="#">CSCwh12619</a>	"Routing DNA Essentials: Tier 0: 05M" is not available to choose in Cisco SD-WAN Manager GUI
<a href="#">CSCwh62321</a>	Cisco SD-WAN Manager 20.12.1 / admintech upload tool is failing.
<a href="#">CSCwh93441</a>	Cisco SD-WAN Manager: Unable to login SSH including ciscotacro/ciscotacrw.
<a href="#">CSCwi21156</a>	SDCI-Azure connection creation fails Error:PublicIpWithBasicSkuNotAllowedOnExpressRouteGateways
<a href="#">CSCwh66310</a>	Intermittently the SSO user with tenantadmin privilege only getting basic access.
<a href="#">CSCwi30235</a>	Issue with accessing Cisco SD-WAN Manager 20.6.6 GUI using upper-case letter on TACACS username
<a href="#">CSCwi04213</a>	On-prem: New cloud services OTP doesn't get updated via API if OTP is already present in db.
<a href="#">CSCwh62306</a>	Cisco SD-WAN Manager DR fails in the event that a vBond is unreachable.
<a href="#">CSCwi05515</a>	DR Replication taking 2 hours for ~100 MB Size
<a href="#">CSCwh18738</a>	Licenses unapplied from License Management in Cisco SD-WAN Manager after DR failover/failback.
<a href="#">CSCwi07172</a>	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
<a href="#">CSCwi72623</a>	Change partition task stuck, during Cisco SD-WAN Manager upgrade activation from 20.12 to 20.14.
<a href="#">CSCwi53711</a>	Cisco Catalyst SD-WAN Controller upgrade from 20.9.4.1-li to 20.12.2-li fails because of CDB boot error.
<a href="#">CSCwf34015</a>	Unable to push template due to "no ip cef distributed"
<a href="#">CSCwb56080</a>	Fail to deploy config group when AAA accounting "start stop" is set to False.
<a href="#">CSCwi16436</a>	Lan Tracker: Configuration are not saved with correct ip address.
<a href="#">CSCwj09144</a>	Cisco SD-WAN Manager    Intermittent request time out while trying to access administration user groups.
<a href="#">CSCwj12763</a>	The ip name-server command not pushed to Cisco IOS XE Catalyst SD-WAN device.
<a href="#">CSCwj12589</a>	Cisco IOS XE Catalyst SD-WAN device- dns-server addresses in dhcp config are pushed in wrong order.
<a href="#">CSCwh02871</a>	Multiple alarms APIs RBAC is not working as expected.
<a href="#">CSCwj09324</a>	Failed to deploy device with Policy Group. Connection event can be set for inspect action only.
<a href="#">CSCwi95474</a>	6 + 6 DR cluster elects replication leader which has no config-db and fails to connect to neo4j
<a href="#">CSCwi99163</a>	The statistics-database stops importing data with reason : Bulk insertion failur
<a href="#">CSCwj34301</a>	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
<a href="#">CSCwh05956</a>	20.12.2: Alarms corresponding to events are not showing up on Cisco SD-WAN Manager for few devices with DR configuration.
<a href="#">CSCwf75967</a>	Cisco SD-WAN Manager Malicious File Upload vulnerability
<a href="#">CSCwh25000</a>	Cannot overwrite a FW security policy with a CLI add on template.
<a href="#">CSCwh11913</a>	SD-WAN workflows ST and MT VNF primary image path is missing additional file path specified in virtual image page.
<a href="#">CSCwf90207</a>	Edit of variables in additional settings is not working.

Identifier	Headline
<a href="#">CSCwf81695</a>	Unable to add more than 30 VPN Interface SVI.
<a href="#">CSCwh84962</a>	Cisco Catalyst SD-WAN Controller withdraws TLOC RIB out after going into GR.
<a href="#">CSCwf98777</a>	Cisco Catalyst SD-WAN Controller policy is not sending the updated TLOC information.
<a href="#">CSCwh22127</a>	Software initiated reboot due to OMPD crash (segmentation fault).
<a href="#">CSCwh32413</a>	Fixed typo in diagnostics log filename.
<a href="#">CSCwd85558</a>	The app-server java process is not initiating in 6 node 20.6 cluster .
<a href="#">CSCwh01870</a>	Template push failed post Cisco SD-WAN Manager upgrade from 20.4 to 20.9 "udp udp-src-dst-port-list source range"
<a href="#">CSCwh24243</a>	Suppress OMP advertisement of stale versioned TLOCs on Cisco Catalyst SD-WAN Controller
<a href="#">CSCwh11629</a>	Template shows out of sync due to control flap caused by hardware Cisco Catalyst SD-WAN Edge device enterprise cert install.
<a href="#">CSCwf50089</a>	Template push fails when ZBFW policy has sequences matching UDP ports 500/4500 in Cisco SD-WAN Manager 20.9
<a href="#">CSCwh26907</a>	Cisco SD-WAN Manager GUI SaaS probe endpoint type URL is not allowing to use "-" character as value.
<a href="#">CSCwf93420</a>	SD-WAN workflows/20.12.2: LAN OSPFv3 IPv4/IPv6: sub-feature parcel failed to be saved.
<a href="#">CSCwh88227</a>	Application list with duplicate name entries in "Group of Interest".
<a href="#">CSCwf95317</a>	Devices are not receiving the preference via the policy in a Multi-Tenant environment.
<a href="#">CSCwh30799</a>	SD-WAN workflows missing nocloud property in payload when checked in Cisco SD-WAN Manager NFV config group UI.
<a href="#">CSCwh48782</a>	TACACS netadmin users are not able to access vshell on 20.12.
<a href="#">CSCwf83985</a>	20.12:AWS-With Pure IPV6 overlay, vbond vpn 0 ge0/0 interface if-oper-status down after power off/on.
<a href="#">CSCwe90415</a>	Massive update for feature template fails.
<a href="#">CSCwh24574</a>	Application SLA traffic policy with base action allow without any match field is ignored.
<a href="#">CSCwf09036</a>	Cisco SD-WAN Manager configures incorrect IKEv2 lifetime for IPSec tunnels.
<a href="#">CSCvt47226</a>	Routes missing on a Cisco Catalyst SD-WAN Edge devices in a graceful-restart scenario.

Identifier	Headline
<a href="#">CSCwf85996</a>	In Multi-Tenant Cisco SD-WAN Manager, Equinix ICGW is stuck in LIVE state, and not changing to ACTIVE state.
<a href="#">CSCwh06082</a>	Unable to create Azure CGW using NVA created from Azure Portal.
<a href="#">CSCwf86315</a>	Error unlocking device configuration mode to CLI mode.

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

Identifier	Headline
<a href="#">CSCwh62321</a>	Cisco SD-WAN Manager_20.12.1 / admintech upload tool is failing.
<a href="#">CSCwh02871</a>	Multiple alarms APIs RBAC is not working as expected.
<a href="#">CSCwf34015</a>	Unable to push template due to "no ip cef distributed".
<a href="#">CSCwh69041</a>	20.13:SDCI connection using Multicloud TGW marked as success / traffic fails.
<a href="#">CSCwb56080</a>	Failed to deploy configuration group when AAA accounting "start stop" is set to False.
<a href="#">CSCwh87880</a>	The usage of policy group for security configuration has random push error.
<a href="#">CSCwh62306</a>	Cisco SD-WAN Manager DR fails in the event that a Cisco Catalyst SD-WAN Validator is unreachable.
<a href="#">CSCwh28301</a>	Cisco SD-WAN Manager GUI becomes very slow when a large template with 1000+ variables is uploaded.
<a href="#">CSCwh97370</a>	The NAT DIA interface < name>; overload egress-interface < interface>; 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
<a href="#">CSCwe95606</a>	Double GR_Additional log enablement defect
<a href="#">CSCwf68955</a>	Cisco SD-WAN Manager Log Poisoning bypass
<a href="#">CSCwf68959</a>	Cisco SD-WAN Manager Audit Log CSV payload injection
<a href="#">CSCwe66540</a>	Cisco Catalyst SD-WAN : Decommissioning or deleting device did not release the license.
<a href="#">CSCwe95368</a>	- AAR Default SLA values changing by the system
<a href="#">CSCwf68886</a>	Cisco SD-WAN Manager deletes the custom folder whenever editing the IPS settings

Identifier	Headline
<a href="#">CSCwf48674</a>	Cisco IOS XE Catalyst SD-WAN device unified security policy template fails to enable geo database
<a href="#">CSCwf98724</a>	20.11/12 ST/MT: updating app server logo via nms command is not working
<a href="#">CSCwf21372</a>	Cisco SD-WAN Manager does not recognize the resource group for resource group admin login via TACACS
<a href="#">CSCwf63511</a>	OSPFv3 - "Advertise" command not appearing on OSPFv3 for IPV4 address-family
<a href="#">CSCwe85177</a>	Scroll up or down under feature template box change the values.
<a href="#">CSCwe83858</a>	Unable to update DHCP Tunnel interface template if template was cloned from factory default template
<a href="#">CSCwe42158</a>	Cisco SD-WAN Manager GUI : Incorrect Average Values for Latency/Jitter/Loss percentage for Edge Routers
<a href="#">CSCwe57259</a>	Template pushed with wrong APN settings, Cisco SD-WAN Manager shows wrong APN config even after rollbacked.
<a href="#">CSCwe91258</a>	Wireless Template cannot be attached to a C1113-8PLTELAWZ device
<a href="#">CSCwe88453</a>	Cisco SD-WAN Manager not including net mask for BGP for a /32
<a href="#">CSCwf10147</a>	Topology API showing only data links on Cisco Edge devices
<a href="#">CSCwe76283</a>	Cloud Gateway Attachment is not shown for dedicated mode after tag is unmapped
<a href="#">CSCwf63112</a>	Unable to edit the user group's created under Administration &gt; Manage Users.
<a href="#">CSCwf03555</a>	Cisco SD-WAN Manager unable to parse certain timezones and is triggering certificate installation process
<a href="#">CSCwf45552</a>	Cisco Catalyst SD-WAN CoR for SaaS - Enable O365 Application Error
<a href="#">CSCwf51992</a>	Need to hide/remove "key" field in TACACS server configuration in AAA template
<a href="#">CSCwd90586</a>	Cisco SD-WAN Manager scrollbar is executing several API calls that slow down the performance
<a href="#">CSCwe53624</a>	Cisco SD-WAN Manager: cURL may flag error on ca cert file "Error in the time fields of certificate"
<a href="#">CSCwe31281</a>	20.9 Autotunnel Isec tracker:Tracker does not come up at all on vedge
<a href="#">CSCwd54278</a>	aaamgr process restarts unexpectedly
<a href="#">CSCwf67622</a>	Cisco SD-WAN Manager is loading continuously when a new user access is created with Network Hierarchy.
<a href="#">CSCwf63504</a>	OSPFv3 - "distance" command not showing under address-family ipv4

Identifier	Headline
<a href="#">CSCwe87281</a>	Cisco SD-WAN Manager pushing DH group (14,15,16) for SIG template for IKEv2 (unsupported by Umbrella)
<a href="#">CSCwf49674</a>	Cisco SD-WAN Manager is modifying load_balance.json leading to the edges to be disconnected.
<a href="#">CSCwe63222</a>	Certificate output is not getting changed on renew when Cloud Certificate Authorization is Automated
<a href="#">CSCwf28362</a>	Cisco SD-WAN Manager is not generating alarm notifications to be sent to Webhooks server.
<a href="#">CSCwf34096</a>	168 Cisco vEdge 5000 device inbuilt certificate expiring on 12th Nov 2023
<a href="#">CSCwd46383</a>	Cisco SD-WAN Software Denial of Service Vulnerability

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

Identifier	Headline
<a href="#">CSCwf82106</a>	20.10 20.11- Localhost can't be modified to IP in Cluster management Page : GRPC error CO for ZK
<a href="#">CSCwh02871</a>	Multiple alarms APIs RBAC is not working as expected
<a href="#">CSCwh16392</a>	20.12-Tacacs server configuration broken for cloud-init config
<a href="#">CSCwh06082</a>	Unable to create Azure CGW using NVA created from Azure Portal
<a href="#">CSCwh24574</a>	Application SLA Traffic Policy with Base Action Allow without any match field is ignored
<a href="#">CSCwf98976</a>	Cannot save application priority & SLA profile if intf value from drop down list is used first time
<a href="#">CSCwh18738</a>	Licenses unapplied from License Management in Cisco SD-WAN Manager after DR failover/failback
<a href="#">CSCwf85996</a>	In Multi-Tenant Cisco SD-WAN Manager, Equinix ICGW is stuck in LIVE state, not changing to ACTIVE state
<a href="#">CSCwh24857</a>	Cisco SD-WAN Manager UI should show the error when Upper case letter present in " User Group Name"
<a href="#">CSCwh24921</a>	17.12 OGREF: Add Cisco SD-WAN Manager restriction for OGREF toggle
<a href="#">CSCwh24577</a>	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

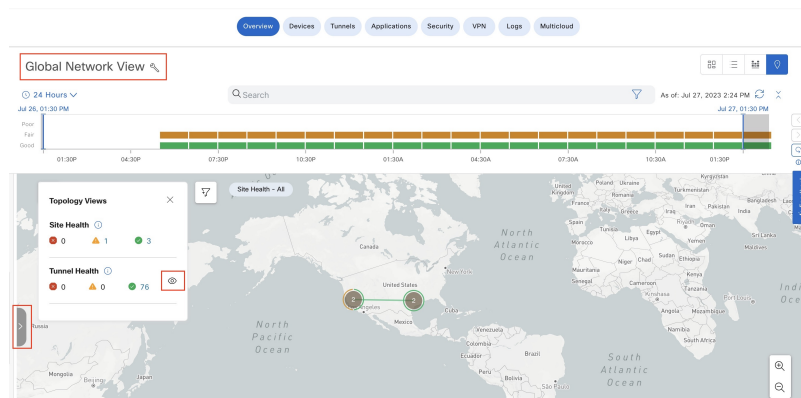
This section presents a comparative summary of the significant GUI changes between Cisco vManage Release 20.11.1 and Cisco Catalyst SD-WAN Manager Release 20.12.1.

### 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](#).

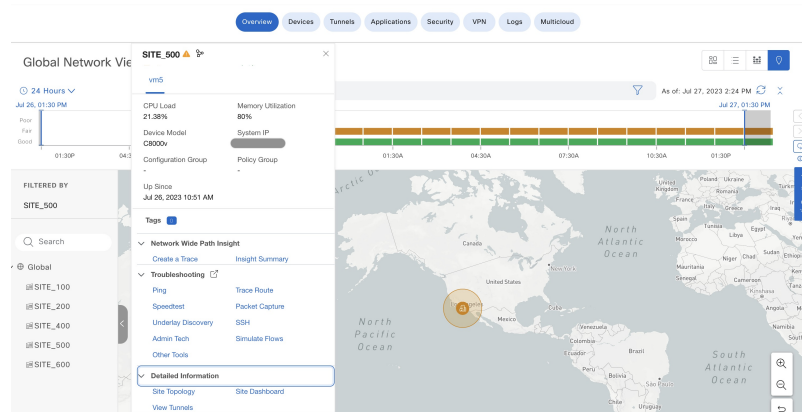
- The **Global Topology** view is called as **Global Network View** in Cisco SD-WAN Manager.

**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.

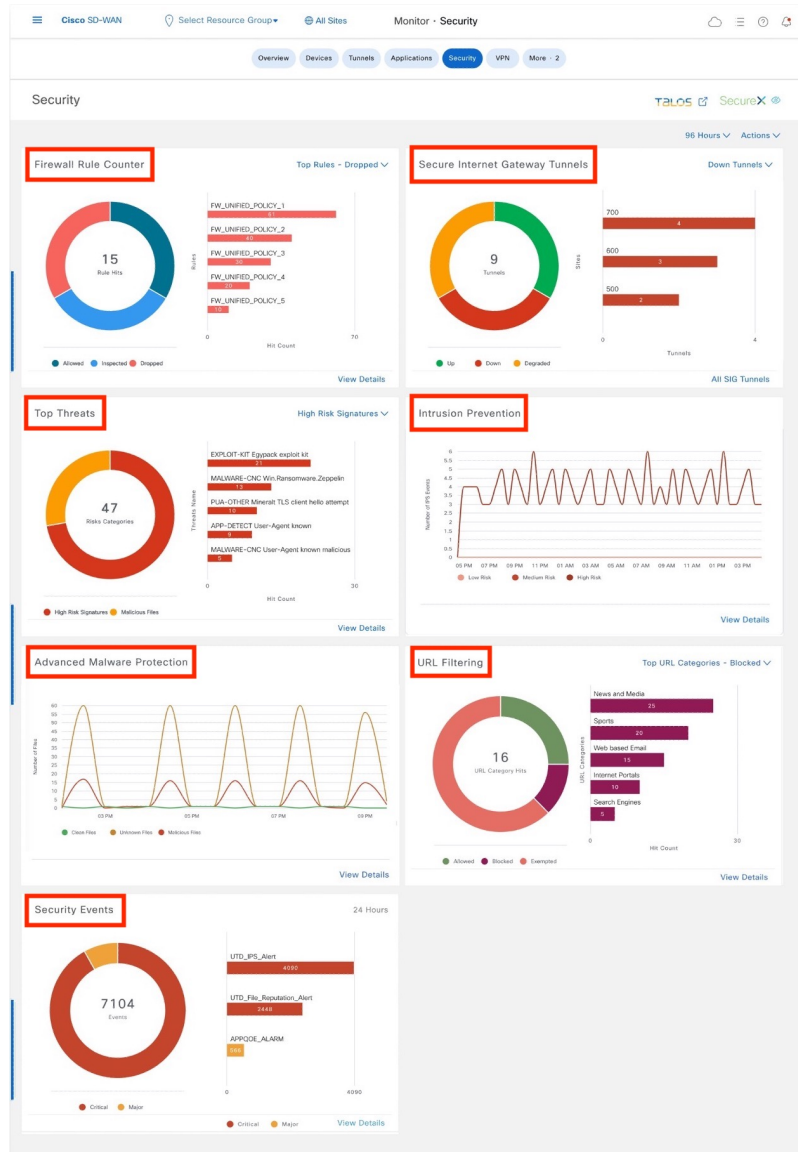
**Figure 2: Device Details for the Selected Site in Global Network View**



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



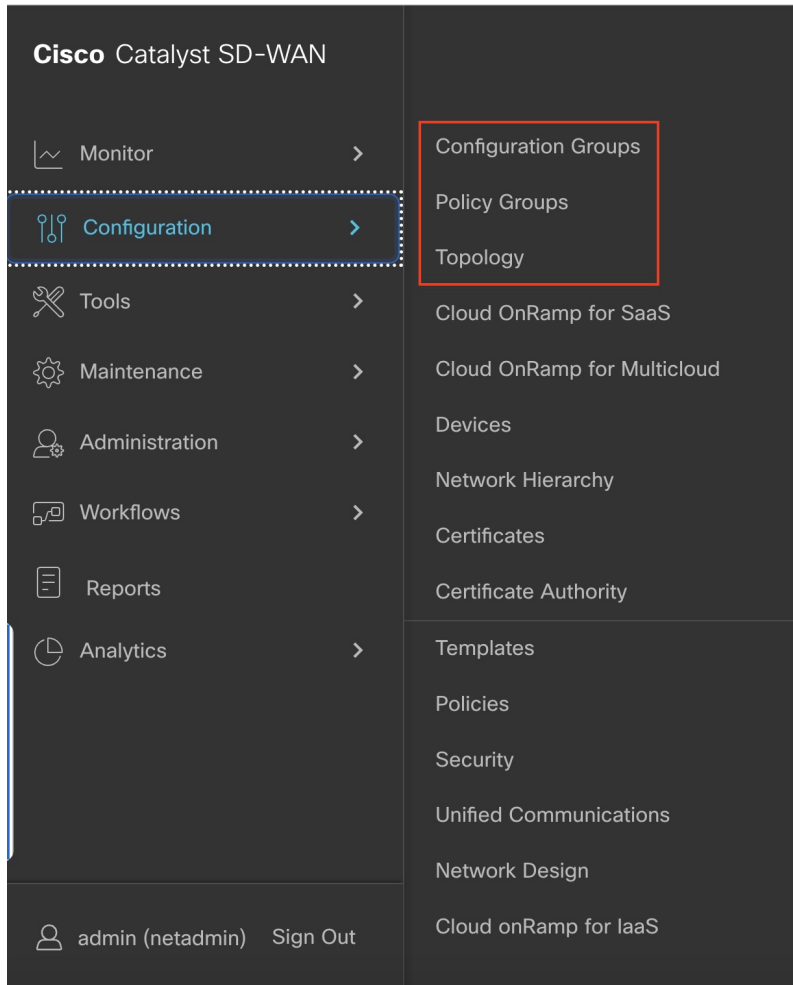
Figure 3: Enhancements to the Security Dashboard Through Modified Dashlets in the Monitor - Security Page



### Configuration Page

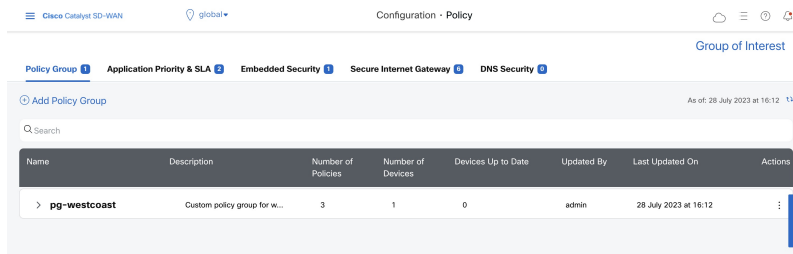
New submenus are added to the **Configuration** menu in Cisco Catalyst SD-WAN Manager menu.

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



## 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**

The screenshot shows the Cisco SD-WAN Manager interface with a slide-in help pane open. The main content area displays a table for 'Device Templates' with columns for Name, Description, Type, Device Model, and Device Templates. The table is currently empty, showing 'No data available'. The help pane, titled 'Feature Templates', contains explanatory text and a table of actions.

**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.

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	<ul style="list-style-type: none"> <li><b>All:</b> Displays both the Default and the Non-Default templates.</li> <li><b>Default:</b> Factory-default templates shipped with the Cisco vManage.</li> <li><b>Non-Default:</b> Customized templates created by a user.</li> <li><b>System Generated:</b> Templates created by the system.</li> </ul>
...	<ul style="list-style-type: none"> <li><b>Edit:</b> Edit a device non-default feature template.</li> <li><b>View:</b> View the factory-default configuration for a feature template.</li> <li><b>Delete:</b> Delete a feature template.</li> <li><b>Copy:</b> Copy a default feature template.</li> <li><b>Change Resource Group:</b> Change the resource group of a device template.</li> <li><b>Change Device Values:</b> Change the</li> </ul>

## 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...

**Overview**

CONTROLLERS	1 vBond	2 vSmart	1 vManage
WAN Edges	5 Reachable		
CERTIFICATE STATUS	0 Warning		
LICENSING	0 Assigned	5 Unassigned	
REBOOT	0 Last 24		

**Site Health** (24 Hours, Good Performing Sites)

4 Sites

**Tunnel Health**

76 Tunnels

**Online Documentation**

**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 CoE 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.

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?

Enter your message...

**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

For any other questions open a request via our [Cisco.com Support Case Manager](#).

Help Contact Feedback

## 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

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](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

---

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT 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](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

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