Release Notes for Cisco Catalyst SD-WAN Control Components Release 20.13.x

First Published: 2023-12-18

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 20.13.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 20.13.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 17.13.x.

What's New for Cisco Catalyst SD-WAN Control Components Release 20.13.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 20.13.1

Feature	Description
Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide	
Cellular Gateway Configuration Using a Configuration Group	Added support for configuring cellular gateways using configuration groups. A new Create Cellular Gateway Group workflow creates a configuration group specifically for cellular gateways.

Feature	Description
Co-Management: Granular Role-Based Access Control	This feature introduces role-based access control (RBAC) based on sites, scope, or roles. It is a method of authorizing system access for users based on a combination of role and scope of a user. You can create scope, users and roles with required read and write permissions for Cisco SD-WAN Manager policies. RBAC prevents unauthorized access and reduces the risk of data breaches and other security incidents.
Remote Logging Over TCP and TLS in Cisco Catalyst SD-WAN Control Components	Added support for remote logging of syslog messages through TCP and TLS. This feature is now extended to include Cisco Catalyst SD-WAN Control Components (Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Manager), in addition to the previously supported Cisco IOS XE Catalyst SD-WAN devices.
Recommended Computing Resources for Cisco Catalyst SD-WAN Control Components Release 20.13.x	
Multitenant Support with Single Node of Cisco SD-WAN Manager	This feature introduces support for a single node large Cisco SD-WAN Manager instance that can include maximum of 24 tenants and 1000 devices.
Cisco Catalyst SD-WAN Monitor and Maintain	
Explore Menu Option	An Explore page provides quick access to various Cisco resources relevant to specific job roles—**NetOps**, **SecOps**, **AIOps**, and **DevOps**. The resources include developer guides, APIs, Cisco DNA Center, Cisco ThousandEyes, and more, in a single pane of glass.

Table 2: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started	
Support for the TLS 1.3 Protocol for Cisco Catalyst SD-WAN Control Connections	This feature adds support for the Transport Layer Security (TLS) 1.3 protocol for Cisco Catalyst SD-WAN control connections.
Configure Third-pary CA Certificates to Cisco IOS XE Catalyst SD-WAN Devices using Cisco SD-WAN Manager	Directly upload CA (Certificate Authority) certificates to Cisco SD-WAN Manager and manage the certificates. This feature makes certificate management simpler, you just select the CA certificate file from your device and upload to Cisco SD-WAN Manager ensuring secure communication and data transfer over the network.

Feature	Description
Enhancements in License Management	Updated license management as follows: Moved selection of license type from license synchronization to license assignment. Added preview of existing template when selected during license assignment. Removed Mixed mode from license types. Added ability to view devices associated with a template and delete a template.
Specify a Region and Subregion When Deploying a Device	You can specify both a region and a subregion when deploying a device.
Cisco Catalyst SD-WAN Security	
Cisco Secure Access Integration	Cisco Secure Access is a cloud security Secure Service Edge solution, that provides seamless, transparent, and secure Direct Internet Access (DIA). This feature supports Cisco Secure Access integration through policy groups in Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN Cloud OnRamp	
Add Cloud OnRamp for SaaS support for loopback, dialer, and subinterfaces	This feature extends the Cloud OnRamp for SaaS support to SD-WAN supported WAN interfaces that includes loopback, dialer, and subinterfaces. It also adds support for TLOC-extension and SIG on loopback, dialer, and subinterfaces.
Option to exclude data prefixes from Cloud OnRamp for SaaS optimization	This feature allows you to define IP prefixes that you want to exclude from being treated for Cloud OnRamp for SaaS optimization.
Enable faster failover by associating a DIA tracker with Cloud OnRamp for SaaS	This feature allows you to associate a tracker with Cloud OnRamp for SaaS for a DIA or gateway site that detects a failed interface faster than Cloud OnRamp for SaaS probing.
AWS Cloud WAN Integration with Dynamic Routing	This feature is an enhancement to the AWS Cloud WAN integration to support site to site communication using dynamic routing.
Cisco Catalyst SD-WAN AppQoE	
SSL Proxy Support for TLS 1.3	With this feature, SSL proxy in AppQoE supports the TLS protocol version 1.3.
Cisco Catalyst SD-WAN Monitor and Maintain	

Feature	Description
Generate Admin-tech File with the Feature Filter	This feature enhances the admin-tech file to generate or collect more detailed feature specific information. The feature-specific technical information is generated in addition to the regular information using the tech filter. The admin-tech file can collect more detailed feature-specific information with the tech feature filter. For example, you can generate separate folders in the admin tech file for IPsec and security policy, which can be helpful when troubleshooting.
Network-Wide Path Insight Integration with Cisco Identity Services Engine	When Cisco Identity Service Engine is integrated with Cisco Catalyst SD-WAN, this feature enables traces to provide the identity of users who send traffic to and receive traffic from applications.
IPv6 support in Cisco SD-WAN Manager UI Troubleshooting	Added support for using an IPv6 address when pinging a device. Also added support for using an IPv6 address when running a traceroute, configuring packet capture, and simulating flows.
Cisco Catalyst SD-WAN NAT	
ICMP Endpoint Tracker for NAT DIA for IPv4 or IPv6 Interfaces	This feature allows you to configure an ICMP endpoint tracker over a DIA path. You can configure the ICMP tracker for NAT DIA on IPv4 or IPv6 endpoints. You can configure ICMP tracker using the **Tracker** or the **IPv6 Tracker** features under transport profile in configuration groups.
Support to automatically configure IPv6 address on a WAN interface by using SLAAC with a Router Advertisement (RA) prefix.	You can configure the Stateless Address Autoconfiguration (SLAAC) by using the RA prefix to automatically assign IPv6 addresses for NAT66 prefix translations.
Support for Flow Stickiness	Flow stickiness records the flow level state of the NAT path and ensures that the application flows don't get reset due to a change in the NAT path. When the first packet match fails in deep packet inspection (DPI), the Edge router ensures the first flow for this unknown application to stick to the original path, bypassing the policy to change the path when it is recognized by the DPI engine a few packets later.
Support for Centralized data policy for NAT66 DIA.	You can configure the Centralized data policy by using the `nat use-vpn 0` command, which ensures that matching traffic is sent to VPN 0 after the source IP is translated, based on the policy match criteria. This feature is supported from service and from tunnel. The fallback option ensures that the traffic falls back to routing and takes the overlay path when the DIA route is not available.
Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)	

Feature	Description
Specify Path Type Preference with Restrict Mode	With this feature, the preferred color group action in app-route and data-policy has additional color-restrict option available to restrict traffic to configured colors. With this option, if multi tiered preferred colors are not available then, the traffic is dropped.
Management Region	A management region is a specialized region that can span all access regions in a Multi-Region Fabric architecture. A management region enables hub-and-spoke connectivity between any router in the network and one or more management gateways. Connectivity between a router and a management gateway uses access region transport services. The connectivity does not use the core region transport service, even when the router and management gateway are in different access regions.
Configure Multi-Region Fabric and Related Features Using Configuration Groups	Configure Multi-Region Fabric features, such as role, region, and so on, and configure transport gateway path behavior on routers, using configuration groups.
Cisco Catalyst SD-WAN Policy Groups	
Configure Traffic and Flow Visibility for Application Priority and SLA policy	This feature allows you to configure additional settings to enable traffic and flow visibility for the application priority and SLA policy in Cisco Catalyst SD-WAN. After you have configured the Cflowd collector in the Network Hierarchy menu in Cisco SD-WAN Manager, you can monitor application and traffic flow over IPv4, IPv6, or both networks at the global hierarchy level.
Configure Secure Service Edge	This feature supports Secure Service Edge configurations for Cisco Secure Access as provider.
Application Catalog	The **Application Catalog** feature provides visibility and identification for applications running in your network environment. The Application Catalog is continuously updated as new applications are developed and existing ones are updated, ensuring that your Cisco SD-WAN Manager environment can adapt to changes in application use. The Cisco SD-WAN Manager integrates Kubernetes cluster discovery and monitoring to monitor your network infrastructure and your containerized applications from a single interface. The feature streamlines the monitoring of your network and applications while providing superior visibility and control.
Cisco Catalyst SD-WAN Systems and Interfaces	
Migration of a Tenant from a Multitenant Overlay to a Single-Tenant Deployment	This feature supports the migration of a tenant from a multitenant overlay to a single-tenant deployment. To migrate a tenant between two Cisco Catalyst SD-WAN deployments, move the tenant configurations, statistical data and WAN edge devices from one deployment to another.

Feature	Description
Support for EtherChannels on the Transport Side	Adds support for configuring EtherChannels on the transport side of a Cisco IOS XE Catalyst SD-WAN device. This feature also introduces support for aggregate EtherChannel Quality of Service (QoS) on the transport side. By combining EtherChannel and QoS, you can optimize network utilization, enhance performance, and maintain quality for specific traffic types. **Note** This feature has limited availability.
Co-Management: Granular Role-Based Access Control	This feature introduces role-based access control (RBAC) based on sites, scope, or roles. It is a method of authorizing system access for users based on a combination of role and scope of a user. You can create scope, users and roles with required read and write permissions for Cisco SD-WAN Manager policies. RBAC prevents unauthorized access and reduces the risk of data breaches and other security incidents.
IP DHCP Smart-Relay	This feature allows the DHCP relay agent to set the gateway address to the secondary IP address when there is no DHCPOFFER message from the DHCP server. A DHCP relay agent is any host or IP router that forwards DHCP packets between clients and servers. This functionality is useful when the DHCP server cannot be configured to use secondary pools.
Support for Traffic Flow Collectors	This feature enables you to configure traffic flow collectors such as the Cflowd server and security logging server. Cflowd monitors service side traffic flowing through Cisco Catalyst SD-WAN devices in the overlay network and exports flow information to the collector. Security logging allows the security logging server to collect and export the syslogs and provides an option to specify a server for high-speed logging (HSL). You can configure the traffic flow collectors by navigating to **Configuration** > **Network Hierarchy** > **Collectors**.
Cisco Catalyst SD-WAN Segmentation Configuration Guide	
Added Support for 2,000 VRFs	Increased support from 300 VRFs to 2,000 VRFs in the overlay network, with up to 500 for a single device.
Cisco Catalyst SD-WAN High Availability Configuration Guide	
Disaster Recovery Reliability Improvements Phase 1	This feature removes the **Pause Replication** button from the **Disaster Recovery** screen. Replication pauses automatically when you pause disaster recovery and resumes when you resume disaster recovery.

Software and Hardware Behavior Changes in Cisco Catalyst SD-WAN Control Components Release 20.13.x

Software and Hardware Behavior Changes in Cisco Catalyst SD-WAN Control Components Release 20.13.1

Behavior Change	Description
On the **Network Hierarchy and Resource Management** page, this release introduces a distinction between access regions and secondary regions.	See the Restrictions for Secondary Regions section for more information about how Cisco SD-WAN Manager handles previously configured regions after upgrading to Cisco Catalyst SD-WAN Manager Release 20.13.1.
When upgrading vEdge devices in the overlay network, the rate of a DTLS control session increases to 4000 pps during the upgrade. After the upgrade is complete, the rate is reset to its original value.	See the Best Practices for Software Upgrades section for more information about change in the rate of a DTLS control session when upgrading the vEdge routers.
You can provide feedback about Cisco Catalyst SD-WAN by clicking the Feedback option that is available on the right as a collapsible side bar.	The Cisco SD-WAN Manager GUI Changes describes this behaviour change in detail.
The new Explore menu option opens a page presenting four job roles—**NetOps**, **SecOps**, **AIOps**, and **DevOps**, each of which displays relevant Cisco Catalyst SD-WAN features.	The Cisco SD-WAN Manager Monitor Overview describes this behaviour change in detail.

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Behavior Change	Description
Controller mode for Cisco ASR 1006-X routers containing RP3 module is no longer supported.	The RMA Replacement of the Cisco ASR 1006-X Chassis and RMA Replacement of the Cisco RP3 Module sections describe the behavior change in detail.
The enterprise certificate notifications for Cisco IOS XE Catalyst SD-WAN devices are enhanced to include critical notifications about certificate expiry.	The Support for SNMP Traps on Cisco Catalyst SD-WAN devices section describes the behavior change in detail.
If your system is configured with an SNMP community string that is longer than 15 characters, in some situations SNMP configuration must be reconfigured after upgrading to Cisco Catalyst SD-WAN Manager Release 20.13.1.	The Configure SNMP using Cisco SD-WAN Manager section describes the behavior change in detail.
You cannot update the Cisco Catalyst 8500-12X4QC port configuration to 2 ports of 100GE by using the Flexible Port Speed feature.	The Flexible Port Speed feature describes the behavior change in detail.

Behavior Change	Description
This release ends Cisco Catalyst SD-WAN support for most Cisco ISR 4000 Series Integrated Services Routers, with the exception of the Cisco ISR 4461 router, which is still supported. For the routers no longer supported in this release, Cisco IOS XE Catalyst SD-WAN Release 17.12.x is the last supported release.	The Cisco Catalyst SD-WAN Device Compatibility page shows the supported releases for each model.

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 Catalyst 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).

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**	**20.13.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: **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.x. or Direct upgrade from 20.6.4 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running 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.x. or Direct upgrade from 20.6.4 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running 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.x. or Direct upgrade from 20.6.4 and later releases. For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version							
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x
20.7.x	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Step upgrade from 20.9.x For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.9.x For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.9.x For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.9.x For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version							
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x
20.8.x	Not Supported	Not Supported	Not Supported	Direct Upgrade	Step upgrade from 20.9.x For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.9.x For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.9.x For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade from 20.9.x For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version							
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x
20.9.x	Not Supported	Not Supported	Not Supported	Not Supported	Direct upgrade For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version							
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x
								Direct Upgrade For cluster upgrade procedure using CLI: **request nms configuration-db upgrade** **Note** • We recom the dat size in disk is than o to 5GB the `req nms configu diagno` comma check data ba size. T applica only fo upgrad device runnin SD-WA Manag Releas 20.1.1 later. • If your Cataly SD-WA Manag runnin vMana Releas 20.9.x you ar

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

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

Note To check the free disk space using the CLI,

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

Note The cluster upgrade must be performed using CLI,

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

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

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

Resolved and Open Bugs for Cisco SD-WAN Controllers 20.13.x

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.13.x

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.13.1

Identifier	Headline
CSCwh81907	APN profile password was found in plain text when Cellular profile template was configured
CSCwf98797	Summary page of nfv CG workflows shows value of "color" for the field that is labeled as "Type"
CSCwi00334	The LAN intf name in dual router config group workflow is getting modified after CG creation
CSCwf08690	The NETCONF/SSH fails when FIPS is enabled on Cisco IOS XE Catalyst SD-WAN device
CSCwh04968	Control Session PPS increase and reset during the upgrade for Cisco vEdge devices
CSCwh47706	20.9 Cisco SD-WAN Manager unable to push SNMPv3 template when the "<" character is in the password
CSCwh02439	Cisco SD-WAN Manager - Unable to add devices to Cloud on Ramp for SaaS due to timeout while loading device list
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, vManage will remove CoR
CSCwi21523	WFLYSRV0272: Suspending server due to NON_FIPS_CRYPTO_FEATURE
CSCwh38837	API call for dataservice/management/elasticsearch/index/size/estimate is failing
CSCwf95165	The vdaemon file is incomplete when generating a Cisco SD-WAN Manager admin-tech using GUI
CSCwh29957	The CLI Add-On Temlate's Config Diff shows wrong configuration
CSCwh02871	Multiple alarms APIs RBAC is not working as expected
CSCwh81740	API call (dataservice/device/tloc) retrieve an additional color which is not present on the device
CSCwh46024	Cisco SD-WAN Manager not starting new traces due to high scaled full mesh network
CSCwh88454	App-server stuck in unhealthy state in two of the nodes after upgrade
CSCwh31482	Wildcard common name is not support for SSL Proxy on vManage
CSCwf96777	Cisco SD-WAN Manager alarming for fan down on 8300 device when fans are only in warning state with high RPMs

Identifier	Headline
CSCwi01270	Cannot overwrite a FW security policy with a cli add on template, config is not seen on device
CSCwh11161	Device template fails on 20.6.5.2 due to SNMP community string
CSCwh73776	20.13: Missing control-connection Cli Generation in CG
CSCwh62321	Cisco SD-WAN Manager20.12.1 / admintech upload tool is failing
CSCwi21156	SDCI-Azure connection creation failsAzure Error:PublicIpWithBasicSkuNotAllowedOnExpressRouteGateways
CSCwh44411	Cisco SD-WAN Manager application-server diagnostics is not displaying Disk I/O Statistics for vManage storage
CSCwi04213	On-prem: New cloud services OTP doesn't get updated via API if OTP is already present in db
CSCwh83203	MT: Centralized policy push with overlapping sites is returing success but Cisco SD-WAN Controller rejects it.
CSCwh62306	Cisco SD-WAN Manager DR fails in the event that a vBond is unreachable
CSCwh24335	Manipulate driver of Neo4j and ES to use static logger instead of new logger (Cisco SD-WAN Manager Slowness 20.6)
CSCwh18738	Licenses unapplied from License Management in Cisco SD-WAN Manager after DR failover/failback
CSCwf88882	Enterprise ZTP server vdaemon crashes due to its root-ca.crt file size

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.13.1

Identifier	Headline
CSCwi33594	The DCA folder is piling UP with small files which is exhausting the space
CSCwi07172	The ssh and ntp are enabled by default in config. groups
CSCwh67520	20.13:AWS:Onboarding process Fail on Any Cisco Catalyst 8000V version < than 17.13 - Getting to Out of sync state
CSCwb56080	Fail to deploy config group when AAA accounting "start stop" is set to False
CSCwi23194	Policy Groups 2.0 - Groups of Interest - Creating application difficult to do
CSCwi16436	Lan Tracker: Configuration are not saved with correct ip address.
CSCwi38870	Cisco SD-WAN Controller is not generating any debug logs running 20.12.2
CSCwi14897	RBAC by VPN groups is blocked on UI (verification failed) - multiple issues
CSCwi45974	Unable to save the TACACS Server configuration when using Configuration Groups

Identifier	Headline
CSCwh16901	HSEC license installation from the workflow does not complete.
CSCwi01358	The aaaMgr namespace is not created in one of the Cisco SD-WAN Manager after configuring radius server
CSCwi21322	20.13.1: Azure SD-Routing CoR: Multicloud Monitoring Dashboard is not showing Gateway/VNET/TAG/VPN
CSCwi20779	Soln: retry logic needed for delete tunnel group from Cisco SD-WAN Manager
CSCwi45443	The vdaemon file is incomplete when generating a Cisco SD-WAN Manager admin-tech using GUI

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 20.13.x APIs, see Cisco SD-WAN Manager API.

Cisco Catalyst SD-WAN Manager GUI Changes

The following are significant GUI updates in Cisco Catalyst SD-WAN Manager Release 20.13.1.

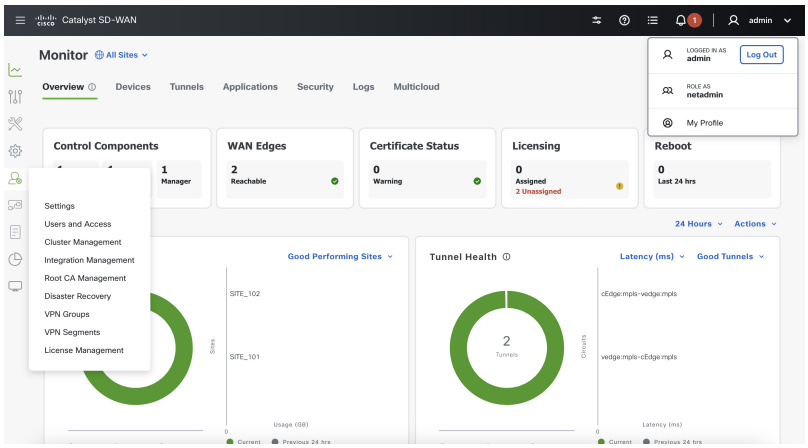
Enhanced Dashboard Experience

The Cisco Catalyst SD-WAN Manager Release 20.13.1 GUI is now updated, based on the Cisco design system, which enhances the look and feel of the dashboard. This upgrade offers a unified experience across various other Cisco products by maintaining consistent design and theme elements.

Some of the significant changes are as follows:

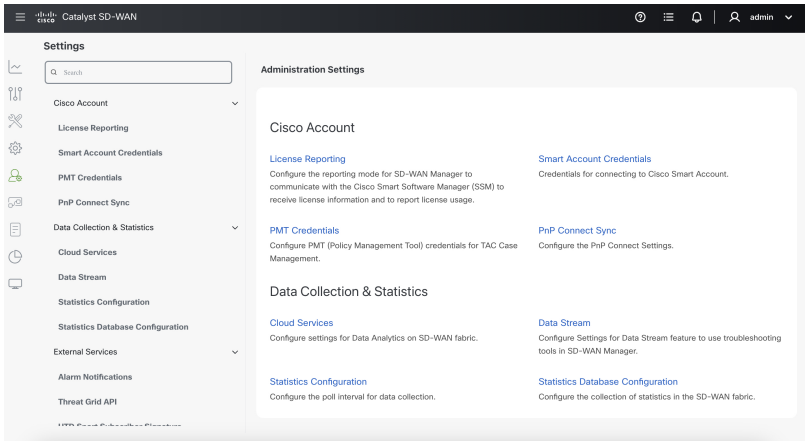
- Monitor Overview page:
  - The navigation panel with menu icons is visible on the left pane. Hover over an icon to view the title or click the hamburger icon to expand the menu options.
  - The **Select Resource Group** option is deprecated.
  - The **Profile** drop-down menu in the top right of the dashboard includes the **My Profile** and the **Log Out** options.
  - In multitenant mode, a **Select Tenant** drop-down list is available at the top-left.

Figure 1: Enhanced Monitor - Overview Page in Cisco Catalyst SD-WAN Manager Release 20.13.1



- **Administration** > **Settings** page - The settings are categorized as follows:
  - **Cisco Account**
  - **Data Collection & Statistics**
  - **External Services**
  - **System**
  - **Trust and Privacy**

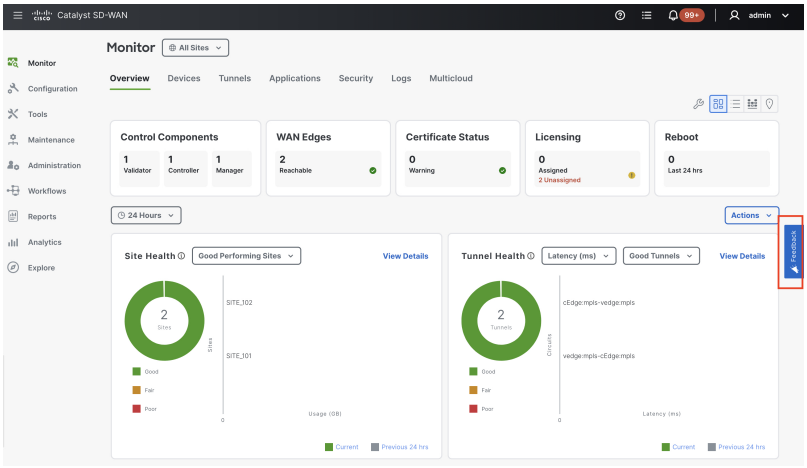
Figure 2: New Settings Layout in the Administration Menu in Cisco Catalyst SD-WAN Manager Release 20.13.1



Feedback About Cisco Catalyst SD-WAN

Starting from Cisco Catalyst SD-WAN Manager Release 20.13.1, you can provide feedback about Cisco Catalyst SD-WAN by clicking the **Feedback** option that is available on the right as a collapsible side bar.

Figure 3: Feedback in Cisco Catalyst SD-WAN Manager Release 20.13.1



You can select a feedback topic from the following options and rate your experience:

- Analytics, monitoring, or troubleshooting
- Software reliability
- Multicloud or security

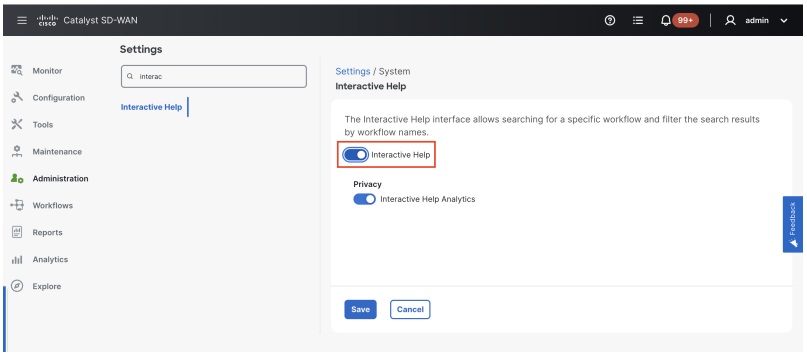
To disable the **Feedback** option, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Navigate to the **System** menu and click **Interactive Help**.
3. Disable **Interactive Help**.

Warning Interactive help setting controls both the **Interactive Help** and the **Feedback** features. Disabling the **Interactive Help** setting disables both the features.

4. Click **Save**.

Figure 4: Administration Settings - Interactive Help in Cisco Catalyst SD-WAN Manager Release 20.13.1

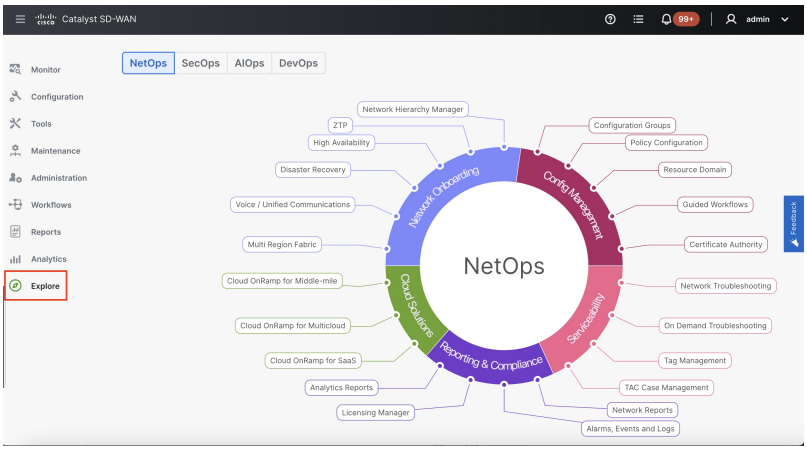


Explore Cisco Catalyst SD-WAN Features Based on Job Roles

In Cisco Catalyst SD-WAN Manager Release 20.13.1, the new **Explore** menu option opens a page presenting four job roles—**NetOps**, **SecOps**, **AIOps**, and **DevOps**. Based on the job role that you choose, the Explore page displays relevant Cisco Catalyst SD-WAN features, along with other Cisco resources such as developer guides, APIs, Cisco DNA Center, Cisco ThousandEyes, and more.

A graphic presents the resources relevant to the job role. For more information, see Explore.

Figure 5: Explore Features Based on Job Roles in Cisco Catalyst SD-WAN Manager Release 20.13.1

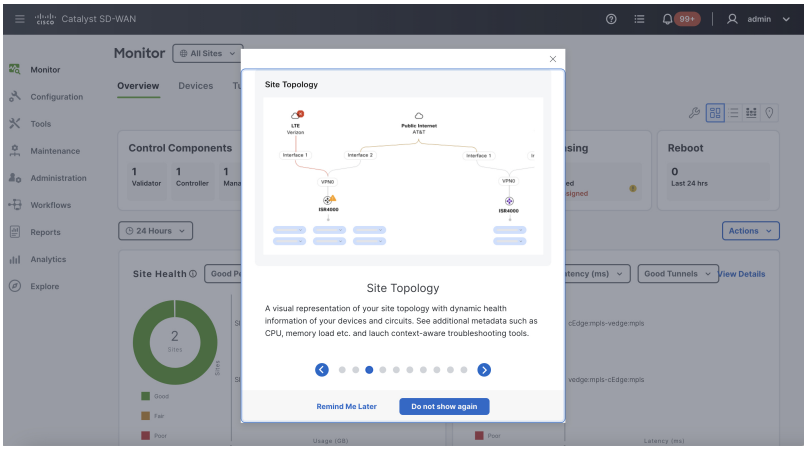


Feature Spotlight

When you log in to Cisco SD-WAN Manager, the **Spotlight** window appears in the overview page, highlighting the new features that are available. The spotlight window displays features along with the feature summary. You can return to the spotlight by clicking the **?** icon in the Cisco SD-WAN Manager menu and choosing **Spotlight**.

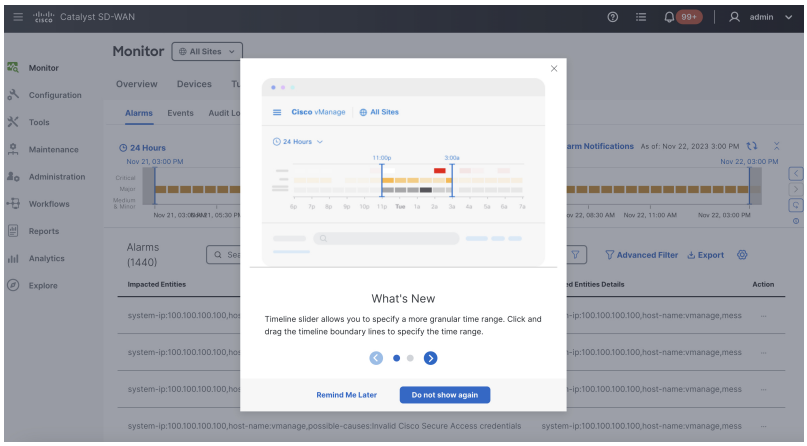
Click **Do not show again** to dismiss spotlight. This action ensures that the spotlight window doesn't appear again.

Figure 6: Spotlight in Monitor - Overview in Cisco Catalyst SD-WAN Manager Release 20.13.1



The spotlight feature is available in other Cisco SD-WAN Manager pages and highlights features specific to that menu. For example, the spotlight in the **Monitor** > **Logs** page displays only two features:

Figure 7: Spotlight in Monitor - Logs in Cisco Catalyst SD-WAN Manager Release 20.13.1

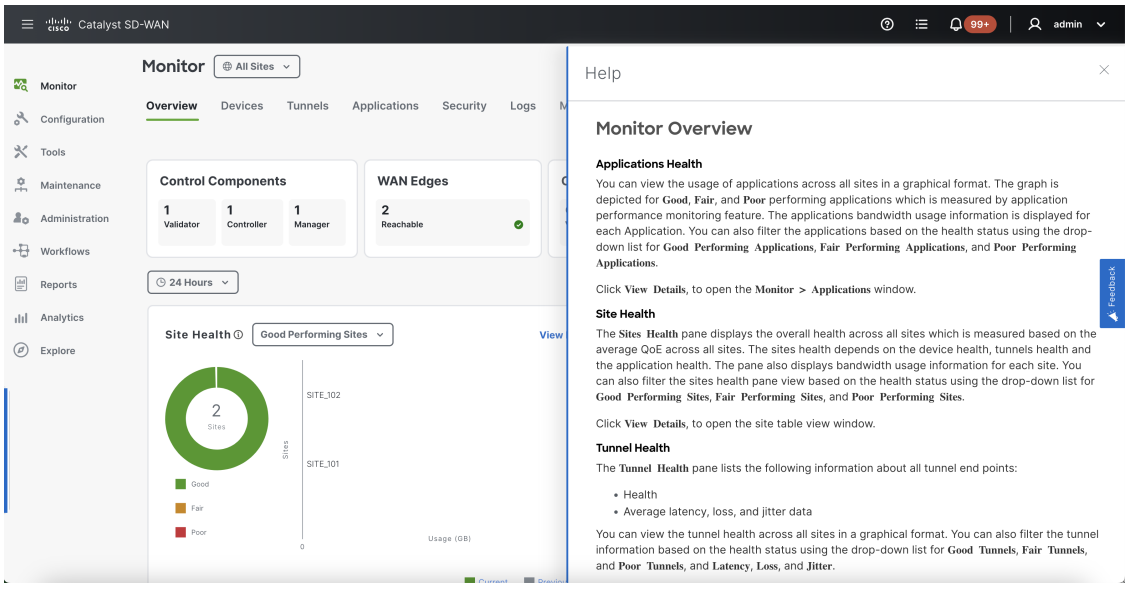


In-product Help

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

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

Figure 8: Help Content in a Slide-in Pane

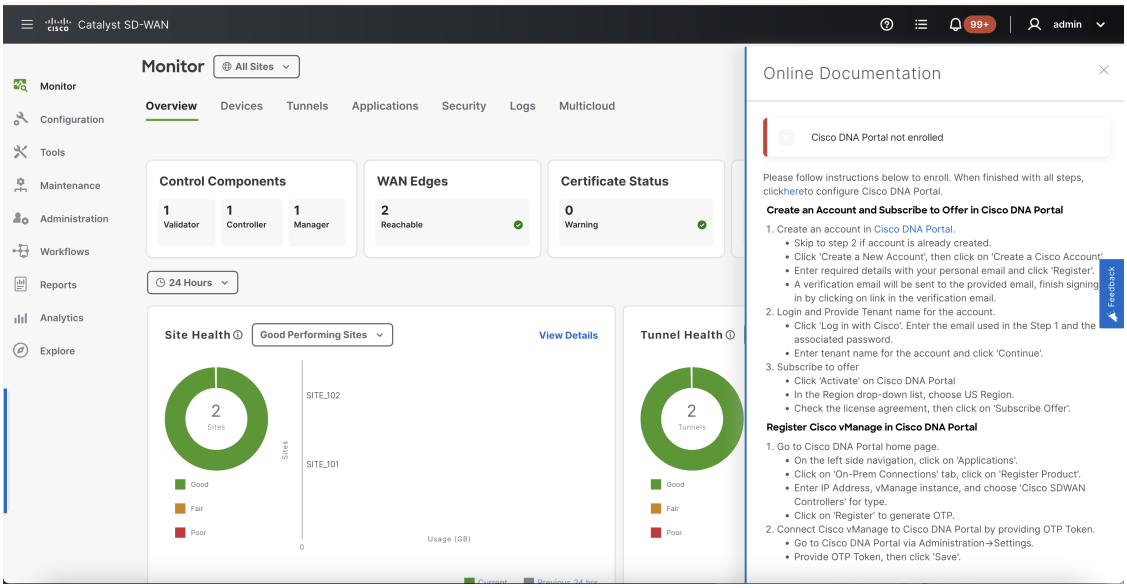


Cisco DNA Sense

Access help content for Cisco SD-WAN Manager UI pages using Cisco DNA Sense by clicking the **?** icon at the top-right corner and choose **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.



Ask Cisco Networking Bot

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

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

Related Documentation

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

Full Cisco Trademarks with Software License