Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.12.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 IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

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 IOS XE Catalyst SD-WAN Release 17.12.1a, 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 IOS XE Catalyst SD-WAN devices.

Related Releases

For release information about Cisco Catalyst SD-WAN Control Components, refer to Release Notes for Cisco SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.12.x

What's New for Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

This section applies to Cisco IOS XE Catalyst SD-WAN devices.

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. For information on additional features and fixes that were committed to the Cisco Catalyst SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

Table 1: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started Guide	

Feature	Description
Support for Certificates Without the Organizational Unit Field	Enterprise certificates that you install on devices do not require the Organizational Unit (OU) field to be defined. Earlier, this field was used as part of the authentication of a device. However, if a signed certificate includes the OU field, the field must match the organization name configured on the device.
Cisco Catalyst SD-WAN Systems and Interfaces	
Cisco Catalyst SD-WAN Remote Access Configuration in SSL-VPN Mode	This feature enables you to configure the following Cisco Catalyst SD-WAN Remote Access features for a device in SSL-VPN mode, using Cisco SD-WAN Manager: — Private IP Pool — Authentication — AAA Policy
Configuration Groups and Feature Profiles (Phase IV)	The following new features are introduced to the feature profiles: — In the System Profile: Flexible Port Speed. — In the Transport Profile: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, T1/E1 Controller — Subfeatures for transport VPN: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, T1/E1 Serial, DSL PPPoE, DSL PPPoA, DSL IPoE, Ethernet PPPoE — In the Service Profile: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, EIGRP Routing, Object Tracker, Object Tracker Group — Subfeatures for service VPN: OSPFv3 IPv4 Routing, OSPFv3 IPv6 Routing, EIGRP Routing, Multilink Controller, Object Tracker, Object Tracker Group — The **Route leak to Global VPN** option is added to the **Route Leak** parameter in the service VPN.
Support for Dual Device Site Configuration	This feature supports dual devices site configuration using configuration groups, for redundancy.
Enhancements to User-Defined Device Tagging	Device tagging has the following new functionalities: — When you add devices to a configuration group using rules, you can choose **Match All** or **Match Any**. — You can use **Starts With** and **Ends With** operator conditions when you add devices to a configuration group using rules. — In addition, the button formerly called **Add New Tag** is now **Create New Tag**.
VFR (Virtual Fragmentation Reassembly) and Underlay Fragmentation	The VFR mechanism reassembles fragmented packets in Cisco Catalyst SD-WAN networks. The packets are fragmented for better transportion and are fragmented while they are travelling through a VFR enabled Cisco IOS XE Catalyst SD-WAN device. Underlay fragmentation fragments packets in the underlying layer of a network. Underlay fragmentation is introduced to easily transport larger packets that exceed the (MTU).

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

Feature	Description
Lawful Intercept 2.0 Enhancements	This feature lets you configure intercepts in the Cisco Catalyst SD-WAN multitenancy mode, and also provides support for Cisco Catalyst SD-WAN Manager clusters.
Enhancements to Flexible NetFlow for vAnalytics	This feature introduces logging enhancements to Cisco Flexible NetFlow for Cisco SD-WAN Analytics. The output of the **show flow record** command has been enhanced for IPv4 and IPv6 flow records.
Enhanced Application-Aware Routing	Without enhanced application-aware routing enabled, Cisco IOS XE Catalyst SD-WAN device require several minutes to switch traffic from one network path to another to meet SLA requirements when the loss, latency, and jitter exceed specific threshold values. Enabling enhanced application-aware routing speeds the detection of tunnel performance issues. This enables Cisco IOS XE Catalyst SD-WAN devices to redirect traffic away from tunnels that do not meet SLA requirements.
Cisco Catalyst SD-WAN Security	
Snort Engine Version Upgrade	This feature adds support for Snort engine version 3, which is an upgrade from version 2.
IPv6 GRE or IPsec Tunnels Between Cisco Catalyst SD-WAN and Third-Party Devices	This feature allows you to configure an IPv6 GRE or IPSEC tunnel from a Cisco IOS XE Catalyst SD-WAN device device to a third-party device over a service VPN.
Enabling MACsec using Cisco SD-WAN Manager	This feature adds support for enabling MACsec using Cisco SD-WAN Manager for Cisco Catalyst SD-WAN devices on the service side. With MACsec enabled using Cisco SD-WAN Manager, communication between devices in the service VPN is protected, thus enhancing security for the service VPN.
OMP Prefixes for IP-SGT Binding	The OMP routes are typically present in the IOS RIB. The OMP routes aren't present in the IOS FIB containing entries that map destination IP addresses to next-hop IP addresses. The IOS FIB operates independently of the control plane, receiving the forwarding instructions from a centralized Cisco SD-WAN Controller instead of consuming the OMP routes from the IOS RIB. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the OMP prefixes get added to the IOS FIB which improves IP-SGT binding.
Cisco Catalyst SD-WAN Cloud OnRamp	
AWS Cloud WAN Integration	AWS Cloud WAN is a managed wide-area network (WAN) service. This feature enables you to easily connect and route remote sites, regions and cloud applications over the AWS global network. You can build and operate the wide-area networks using simple network policies and get a complete view of the global network.

Feature	Description
Added an Azure Instance Type	For the Microsoft Azure West Central US and Australia East regions, added the Standard_D16_v5 Azure instance type, which includes 16 CPU cores and 64 GB of memory. You can deploy this type of instance for SKU scale values of 20, 40, 60, and 80.
Cisco Catalyst 8000V Edge Software Support	You can deploy a Cisco Catalyst 8000v Edge Software as the Interconnect Gateway in the Equinix fabric and connect an Cisco Catalyst SD-WAN branch location to the Interconnect Gateway.
Addition of VPC and VNet Tags to SDCI Connections	You can add or modify additional properties of Virtual Private Cloud (VPC) and Virtual Networks (VNets) tags that are associated with a connection.
Audit Management in Equinix	You can identify the gaps or disconnects between Cisco SD-WAN Manager intent and what is realized in the cloud. The audit management helps in understanding if the interconnect cloud and provider states are in sync with the Cisco SD-WAN Manager state.
Cisco Catalyst SD-WAN Policy Groups	
Policy Groups	This feature provides a simple, reusable, and structured approach for configuring policies in Cisco Catalyst SD-WAN. You can create a policy group, that is, a logical grouping of policies that is applied to one or more sites or a single device at the site in the network. To deploy the policy group to devices, the devices must be managed by a configuration group in Cisco Catalyst SD-WAN. You can configure policies based on features that are required, recommended, or uniquely used, and then combine them to complete a policy configuration.
Security Policy Using Policy Groups	This feature provides a simple, reusable, and structured approach for configuring security policies in Cisco Catalyst SD-WAN. You can create a security policy, that is, a logical grouping of policies that is applied to one or more sites or a single device at the site in the network. To deploy the policy group to devices, the devices must be managed by a configuration group in Cisco Catalyst SD-WAN. You can configure policies based on features that are required, recommended, or uniquely used, and then combine them to complete a policy configuration.
Topology	This feature allows you to provision a **Mesh** or a **Hub and Spoke** topology policy which is applied to Cisco Catalyst SD-WAN Controllers. This allows exchange of data traffic between two or more Cisco IOS XE Catalyst SD-WAN devices.
Cisco Catalyst SD-WAN Monitor and Maintain	
Heatmap View for Alarms	In the heatmap view, a grid of colored bars displays the alarms as **Critical**, **Major**, or **Medium & Minor**. You can hover over a bar or click it to display additional details at a selected time interval. The intensity of a color indicates the frequency of alarms in a severity level.
Heatmap View for Events	In the heatmap view, a grid of colored bars displays the events as **Critical**, **Major**, or **Minor**. You can hover over a bar or click it to display additional details at a selected time interval. The intensity of a color indicates the frequency of events in a severity level.

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

Feature	Description
multi-factor-auth duo command	This command allows you to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in.

New and Enhanced Hardware Features

New Features

- Support for Cisco SM-X-1T3/E3 Module: Cisco SD-WAN Manager CLI device templates now supports Cisco SM-X-1T3/E3 module.

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.12.x

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.12.2

Behavior Change	Description
Added support for certificates that do not have a matching Organizational Unit (OU) field: When onboarding a device, if the associated enterprise certificate has one or more OU fields defined, Cisco Catalyst SD-WAN does not require that any of the OU fields match the organization name of the fabric.	The Configure Enterprise Certificates for Cisco SD-WAN Controllers section describes the behavior.
For all ISR1100 platforms, before changing the resource profile, you must reboot the device. Performing a reboot improves the perfomance of ISR1100 platforms.	The Supported Platforms section in the *Unified Threat Defense Resource Profiles* chapter describes the behavior.
Added an advanced telemetry option to enable Cisco SD-WAN Manager to collect anonymized data for the Cisco Catalyst SD-WAN Data Collection Service (DCS).	The Enable or Disable Cisco Catalyst SD-WAN Telemetry section describes the option.

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

Behavior Change	Description
You cannot include a comma in the **Organization Name** field of the bootstrap configuration file.	The Enable Reverse Proxy and Cisco Catalyst SD-WAN Overlay Network Bring-Up Process sections are updated twith a note on the new behavior.
The **Viptela-User-Group** and **Viptela-Resource-Group** tags are used in RADIUS and TACACs configurations for accounting and authorization.	The Configure the Authentication Order section is updated with a note on new tag definitions.

Behavior Change	Description
A restriction for rebooting a control manage is added.	The Connect Cisco SD-WAN Manager VM Instance to Cisco SD-WAN Manager Console section is updated with the restriction.
Device variable names can contain the following special characters dots (.), forward slashes (/) and square brackets ([]).	The Configure Device Values section is updated with the new support for special characters.
Bar chart to display changes from the previous time period.	The following sections are updated in the Cisco SD-WAN Manager Monitor Overview dashboard with information about the dashlets displaying a bar chart showing the changes from the last time period: • Site Health • Tunnel Health • WAN Edge Health • Application Health
A new command to run diagnostics on a Cisco Catalyst SD-WAN Manager cluster.	The Troubleshooting Commands chapter has been updated with a new command **vdiagnose vmanage cluster**.
Change in the severity value of a few alarms.	The Alarms chapter has been updated with the change in the alarm severity value for the following alarms: • New CSR Generated • Root Cert Chain Installed • Root Cert Chain Uninstalled
New commands that display details of alarms that are generated in Cisco SD-WAN Manager. These commands provide better readability into the alarms.	The Troubleshooting Commands chapter has been updated with the **show sdwan alarms detail** and **show sdwan alarms summary** commands.
In addition to routers in controller mode, from Cisco Catalyst SD-WAN Manager Release 20.12.1, Cisco SD-WAN Manager can monitor routers that are in autonomous mode and not part of the Cisco Catalyst SD-WAN overlay network. These routers appear with the label **SD-Routing** in the **Device Model** column to distinguish them from routers that are part of the overlay network.	Updated the View Controller and Device Information section to describe the new behavior.

Behavior Change	Description
You can configure a global certificate authority using the **Configuration** > **Certificate Authority** option in Cisco SD-WAN Manager. In earlier releases, there was an **Administration** > **Settings** > **Certificate Authority (CA) Settings** option that provided the same functionality, but that option has been removed in this release.	See the Certificate Management section for information about certificates.
You can commit the configuration before rebooting a control manage device through Cisco Catalyst SD-WAN Manager.	The Cisco SD-WAN Manager Console section is updated to describe the new behavior.
In Cisco SD-WAN Manager, **auth-no-priv** authentication algorithm is not supported.	The Configure SNMP on Cisco IOS XE Catalyst SD-WAN Devices section is updated with the support details.
Use the **tools consent-token** command to authenticate the network administrator of an organization to access system shell. Starting Cisco Catalyst SD-WAN Manager Release 20.12.1, the **request support ciscotac** command is deprecated.	The Ciscotac User Access section is updated to describe the new behavior.
Authorization rule for **vshell** is limited to only netadmin users.	The User Authorization Rules table in the Role-Based Access Control chapter is updated with the new rule.
In a Microsoft Azure setup, to allow packets with IPv6 Unique Local Addresses (ULA) on the device, configure the **enable-ipv6-unique-local-address** command to enable or disable these addresses.	The Deploy Cisco Catalyst SD-WAN Controllers in Azure: Tasks section is updated to describe the new behavior.
If multiple Azure Virtual WAN hubs are there in a region, you can select a particular Azure Virtual WAN hub for that region. Once you choose the Azure Virtual WAN hub, all subsequent connections created for Azure Virtual WAN uses the same Azure Virtual WAN hub.	See the Virtual WAN Setting for Megaport and Virtual WAN Setting for Equinix sections for more information.
You have the option to choose to delete Express-Route and vWan at the time of deletion. When you delete a GCP connection, you can optionally select to delete the Google Cloud Router, or manage these resources as required.	See the Delete Connection section for more information.
The Application Monitoring feature is enabled with read and write permission.	See the User Group Permissions:Cisco IOS XE Catalyst SD-WAN devices for more information.
The mutual authentication option is enabled with read and write permission.	See the User Group Permissions:Cisco IOS XE Catalyst SD-WAN devices for more information.

Important Notes, Known Behaviors, and Workarounds

- Cisco IOS XE Catalyst SD-WAN devices with the SFP-10G-SR module do not support online insertion and removal (OIR) of the module.

Resolved and Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.12.x

This section details all fixed and open bugs for this release. These bugs are available in the Cisco Bug Search Tool

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.12.3

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.12.3

Identifier	Headline
CSCwi31523	EPBR FIA is not enabled on port-channel sub-interface.
CSCwi46413	Cisco IOS XE Catalyst SD-WAN device does not install OMP route with high preference using service chaning.
CSCwi27324	Tunnels behind Sym-nat does not come up or flap after "clear omp all" trigger on HUB.
CSCwi44633	Fragmented radius access-request packets are dropped when NWPI is running.
CSCwh72441	The show sdwan appqoe aoim-statistics - APPQOE services restart.
CSCwj15983	MRF: OMP debugs does not print any reason why from another BR in the same region ignored.
CSCwh82168	One of IPSEC IKE tunnel goes down when second IPSEC IKE tunnel has been shut with same source interface.
CSCwi33634	Cisco IOS XE Catalyst SD-WAN device is incorrectly consuming icmp reply packets.
CSCwh65016	Unexpected reboots on Cisco IOS XE Catalyst SD-WAN device due to QFP exception.
CSCwf63771	Non-Fabric:With multiple interfaces in instance, using minimal bootstrap unable to onboard Cisco Catalyst 8000V.
CSCwi33543	SDWAN org name matching one of the OU. This is not needed for Enterprise Certification Mode.
CSCwi05395	The snmpbulkget cannot get loss, latency, and jitter for ProbeClassTable & ClassIntervalTable OIDs
CSCwi32044	Cisco IOS XE Catalyst SD-WAN device reboot due to "Critical process vip_confd_startup_sh".
CSCwi07137	Crash when traffic is sent to UTD.
CSCwh53943	Dialer interface blocking SIG Auto Tunnel workflow.

Identifier	Headline
CSCvr51536	Cisco IOS XE Catalyst SD-WAN device cflowd source interface for non-loopback interface does not get pushed to Cisco IOS XE Catalyst SD-WAN device.
CSCwi49363	confd_cli processes hanging and are maxing out CPU.
CSCwi31747	SymNat with low bandwith is not working.
CSCwi19875	Cisco IOS XE Catalyst SD-WAN device is unable to process hidden characters in a file while trying to use bootstrap method.

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.12.3

Identifier	Headline
CSCwi35716	AAR backup preferred color not working as expected from 17.12.1.
CSCwj14121	The snmpwalk for OID ifOperStatus gives different output before & after upgrade for serial interface.
CSCwh63864	Service-side NAT translation discrepancy.
CSCwf44703	Cisco IOS XE Catalyst SD-WAN device: NAT64 prefix is not originated into OMP
CSCwi58561	Cisco IOS XE Catalyst SD-WAN device : Tracker not working after software upgrade
CSCwi53549	Cisco IOS XE Catalyst SD-WAN device router crash with reason "Critical process fman_fp_image fault on fp_0_0 (rc=134)"
CSCwj02628	Speed-test not working for the Cisco IOS XE Catalyst SD-WAN device running on code 17.12.2.
CSCwh67046	Install UTD image using remoter server with hostname is not working.
CSCwi16015	[SIT]: SSE tunnels don't come up with Dialer interface.Relax check in IKE.
CSCwi62230	SIG tunnel: 'SIG STATEâ is showing blank value.
CSCwf98902	Solution: crash seen on fman_fp / ucode during longevity run (cpp_plu_alloc_v2).

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.12.2

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.12.2

Identifier	Headline
CSCwf94052	BFD going down for newly onboarded Cisco IOS XE Catalyst SD-WAN device.
CSCwh39906	Cisco IOS XE Catalyst SD-WAN device: confd_cli may cause high CPU. Parent PID of "confd_cli" containing "show ip fib".
CSCwf71051	Issues seen due to race conditions between Cisco Catalyst SD-WAN policy and og-mgr on config-change.

Identifier	Headline
CSCwb74384	Cisco IOS XE Catalyst SD-WAN device: confd_cli high CPU utilization after executing "show sdwan app-route stats".
CSCwf84522	Cisco Catalyst 8500L Edge Platform: Unexpectedly rebooted while classifying packet with CTF (Common Flow Table).
CSCwf94294	Misprograming during vpn-list change under data policy.
CSCwf95095	Intermittent BFD session flaps on Cisco IOS XE Catalyst SD-WAN device service side interface.
CSCwh58907	Cisco IOS XE Catalyst SD-WAN device: DNS probes for endpoint-tracker API are sent on wrong interface.
CSCwh67812	Crypto Map feature CLIs are unavailable in 17.12.1

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.12.2

Identifier	Headline
CSCwi00661	The Per-Tunnel QoS policy with loopback as WAN bind mode is not working.
CSCwi00369	Cisco IOS XE Catalyst SD-WAN device lost security parameter after upgrade.
CSCwh63864	Service-side NAT Translation discrepancy.
CSCwh72441	show sdwan appqoe aoim-statistics - APPQOE services restart.
CSCwh76453	The trracker for TLOC extension is down even though TLOC is up and there is ICMP reachability.
CSCwh06870	The APN password is in plain text when cellular controller profile is configured.
CSCwh82168	One of IPSEC IKE tunnel goes down when second IPSEC IKE tunnel has been shut with same source interface.
CSCwh88316	%EVENTLIB-3-CPUHOG: F0/0: fman_fp_image: uipeer downlink listener:
CSCwh65016	There are unexpected reboots on Cisco IOS XE Catalyst SD-WAN device due to QFP exception.
CSCwh67046	The 'Install UTD image' using remoter server with hostname is not working.
CSCwf63771	Non-Fabric:With multiple interfaces in instance, unable to onboard Cisco Catalyst 8000V Edge Software using minimal bootstrap.
CSCwf44703	Cisco IOS XE Catalyst SD-WAN device: NAT64 prefix is not originated into OMP.
CSCwh53943	The Dialer interface is blocking SIG Auto Tunnel workflow.
CSCwf69062	SDRA-SSLVPN : The sslvpn session closes with re-authentication error after some interval of time.

Identifier	Headline
CSCwf95066	17.12 SIG Zscaler IPSec UX2.0: Tracker for Tunnel15000001 is down after source interface swap.
CSCwh95119	The secure-internet-gateway tunnels show no output for generic tunnels.
CSCwf45486	OMP to BGP redistribution leads to incorrect AS_Path Installation on chosen Next-Hop.

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.2.1a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

Identifier	Headline
CSCwf61793	Traceback during policy changes
CSCwf43470	Cisco IOS XE Catalyst SD-WAN device : Traceroute not working with NAT pool configuration
CSCwe43341	TLS control-connections down, traffic from controller dropped with Cisco Catalyst SD-WANImplicitAclDrop
CSCwe18276	17.6: Route-map not getting effect when its applied in OMP for BGP routes
CSCwf38166	CPP Ucode crash when Multicast traffic and UTD is enabled together on the same Cisco IOS XE Catalyst SD-WAN device
CSCwf38281	Misprograming during policy changes
CSCwf14727	FNF ucode crash when add or remove interface
CSCwf39945	Device requested SLAC without customer issuing command
CSCwe38296	The cat8500 Procyon Packets drop due to MACSEC post-encryption padding behavior
CSCwe90501	CSR1000v upgrade fails from 17.3.4a to C8000v 17.6.5 due to "advertise aggregate" with vrf.
CSCwe85195	AAR: BoW feature ignoring color preference from Tiered Transport preference configuration
CSCwf67857	MPLS_NAT_OUTPUT_FIA is not enabled for TLOCs created after SSNAT data policy push
CSCwe81991	The fugazi crash with qfp-ucode-fugazi in C8500L at @posix_mempool_prime_cache
CSCwe65036	[SIT]: Nutella crashed and reboot history shows "IntelResetRequest" on upgrade
CSCwd53710	17.10 - Crash seen when umbrella/zscaler template pushed to device when name_lookup takes > 30 sec
CSCwe70374	Cisco 8300/85000 platform punt-policer is not configurable
CSCwd42523	Same label is assigned to different VRFs

Identifier	Headline
CSCwf49597	Traffic is getting dropped with "Cisco Catalyst SD-WANDataPolicyDrop" with TunnelReason:MATCHED_NONE
CSCwd90056	C8500-12X4QC P2MP WAN MACSEC does not allow traffic to pass on the link
CSCwe70642	AAR overlay actions are applied to DIA traffic
CSCwe85421	Cisco IOS XE Catalyst SD-WAN device BFD Session Down with interface flap
CSCwf21973	Device replying with NAT pool IP address instead of the WAN IP address
CSCwf26771	Invalid L4 Header drop due to multiple encap
CSCwf25249	The AppQoE DRE shows the optimized traffic is more than the original traffic on the data center SCs
CSCwf05980	C8300 dropping Speedtest/IPerf packets with drop reason DROP 19 (Ipv4NoRoute)
CSCwe79007	Cisco IOS XE Catalyst SD-WAN device unexpected reload when doing ips test with UTD ips engine
CSCwe39157	During Soak Run, On C8500L-8S4X, Memif channel's were missing and causing SC-SN state down
CSCwf16608	Cisco IOS XE Catalyst SD-WAN device configured with 10G BDI might reload when running NWPI Trace with QoS Insight enabled
CSCwf38449	SLA violation alarm shows incorrect reading of DSCP value
CSCwf40849	Cisco IOS XE Catalyst SD-WAN device IPv6: removing "advertise aggregate" configuration does not remove the entry from OMP
CSCwe49684	Cisco Catalyst SD-WAN BFD sessions keeps flapping intermittently
CSCwb39206	Enable VFR CLI in Cisco Catalyst SD-WAN mode

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.12.1a

Identifier	Headline
CSCwf94052	BFD going down for newly onboarded Cisco IOS XE Catalyst SD-WAN device
CSCwd98074	OMP keeps advertising route after corresponding OSPF route removed if "advertise network" configured
CSCwh23659	Umbrella Tunnels go to degraded state when default tracker is enabled.
CSCwh08536	F0 Data Plane programming issue
CSCwh04520	Unexpected reload on Cisco IOS XE Catalyst SD-WAN device due to cpp ucode crash
CSCwf80927	Speed tests to internet from C8500 (17.9.3) triggered from Cisco SD-WAN Manager 20.9.3.1 will fail sometimes

Identifier	Headline
CSCwh20577	Crashed by TRACK Client thread at access invalid memory location
CSCwf84522	Cisco IOS XE Catalyst SD-WAN device(C8500L) Unexpected rebooted while classifying packet with CTF (Common Flow Table)
CSCwh06870	APN password in plain text when Cellular controller profile is configured
CSCwh00320	Show run and Show Cisco Catalyst SD-WAN run not in sync after removing GigabitEthernet3 c8000v
CSCwf44703	Cisco IOS XE Catalyst SD-WAN device: NAT64 prefix is not originated into OMP
CSCwf95535	Intf/System xml files are not generated on Cisco IOS XE Catalyst SD-WAN device
CSCwf95095	Intermittent BFD session flaps on Cisco IOS XE Catalyst SD-WAN device service side interface
CSCwf94294	Misprograming during vpn-list change under data policy.
CSCwf71116	Static route keep advertising via OMP even though there is no route.
CSCwf45486	OMP to BGP Redistribution Leads to Incorrect AS_Path Installation on Chosen Next-Hop
CSCwh01318	Multiple Crashes observed on Cisco IOS XE Catalyst SD-WAN device platform due to Memory Exhaustion

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.

Supported Devices

For device compatibility information, see Cisco Catalyst SD-WAN Device Compatibility.

Cisco SD-WAN Manager GUI Changes

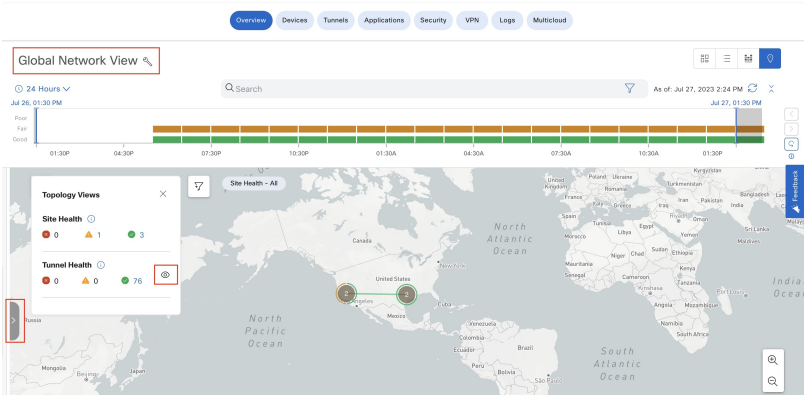
This section presents a comparative summary of the significant GUI changes between Cisco vManage Release 20.11.1 and Cisco Catalyst SD-WAN Manager Release 20.12.1.

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.

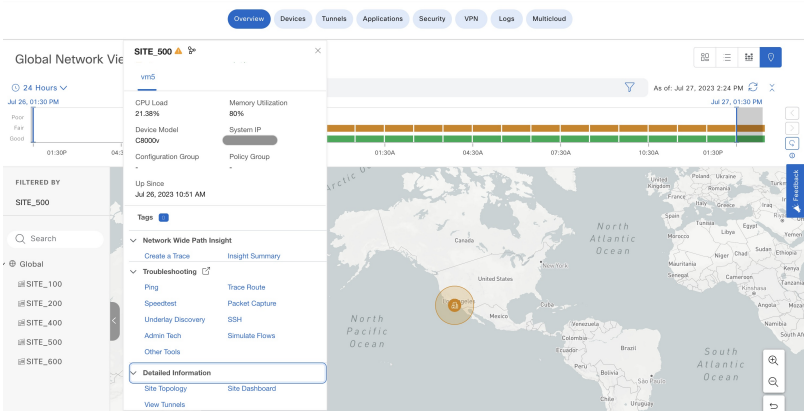
- The **Global Topology** view is called as **Global Network View** in Cisco SD-WAN Manager.

Figure 1: Global Network View in Monitor - Overview Page



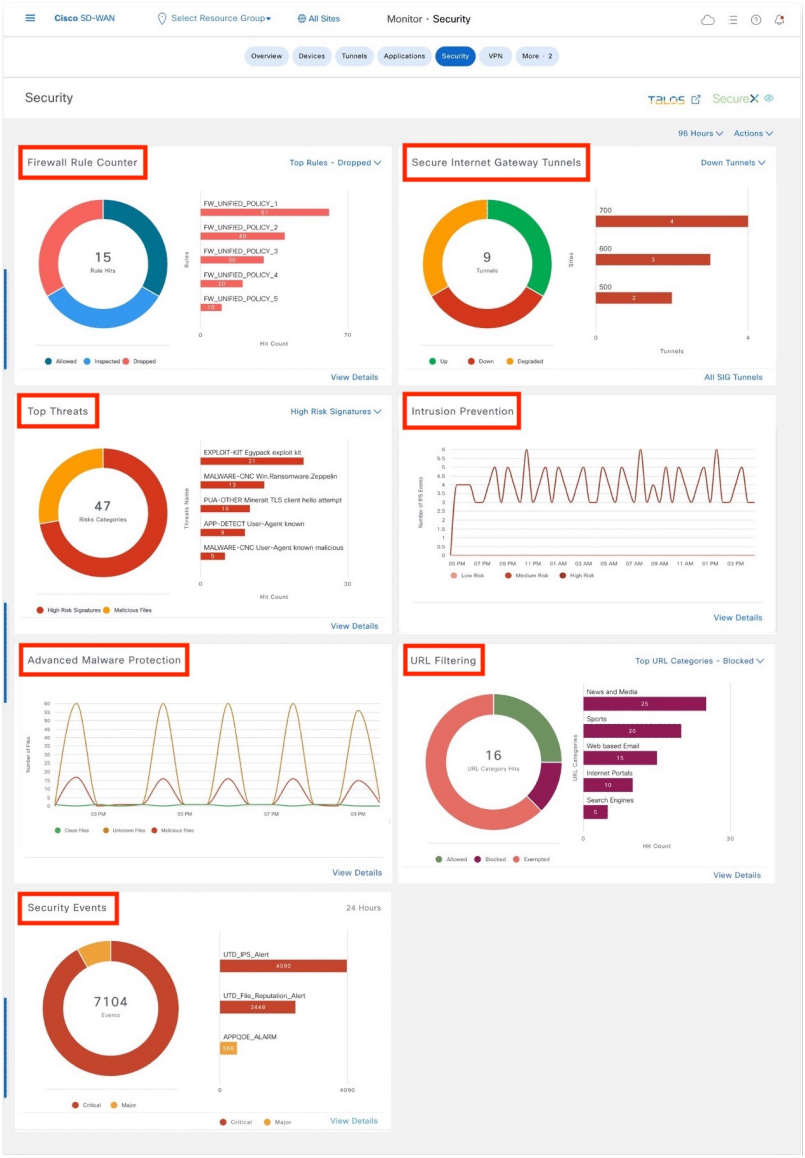
Click the eye icon to view the tunnel connection with aggregated tunnel health between the sites. Click the arrow on the left to open the network hierarchy menu.

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.

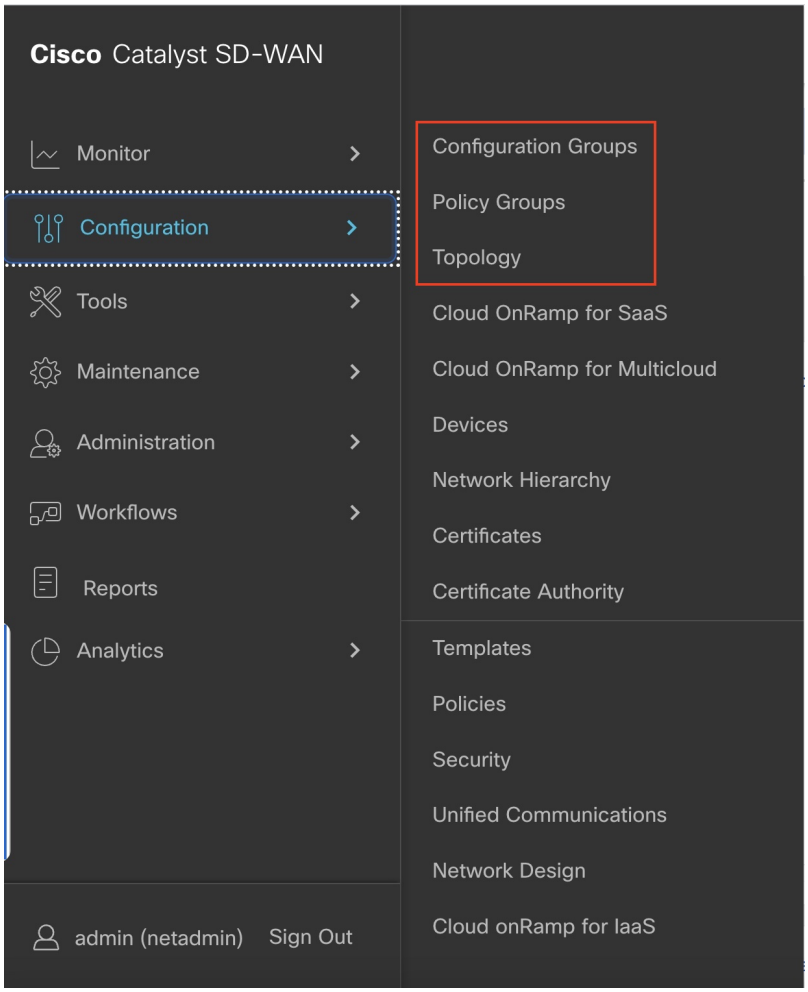
Figure 3: Enhancements to the Security Dashboard Through Modified Dashlets in the Monitor - Security Page



Configuration Page

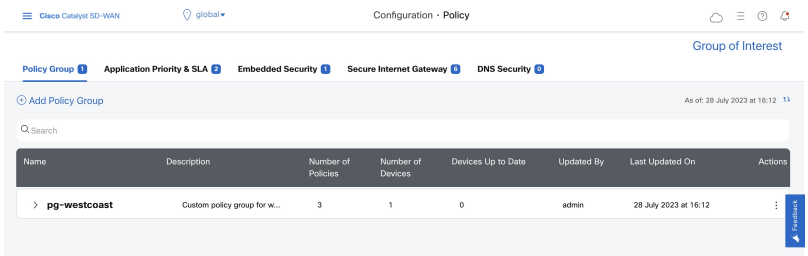
New submenus are added to the **Configuration** menu in Cisco Catalyst SD-WAN Manager menu.

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

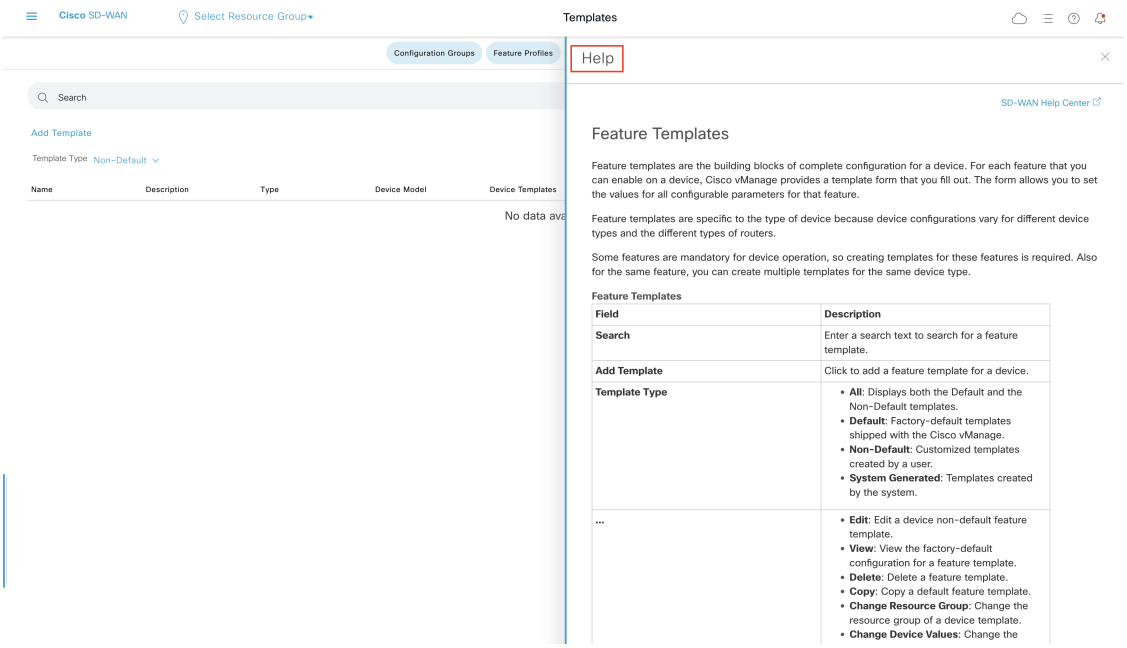


In-product Help

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

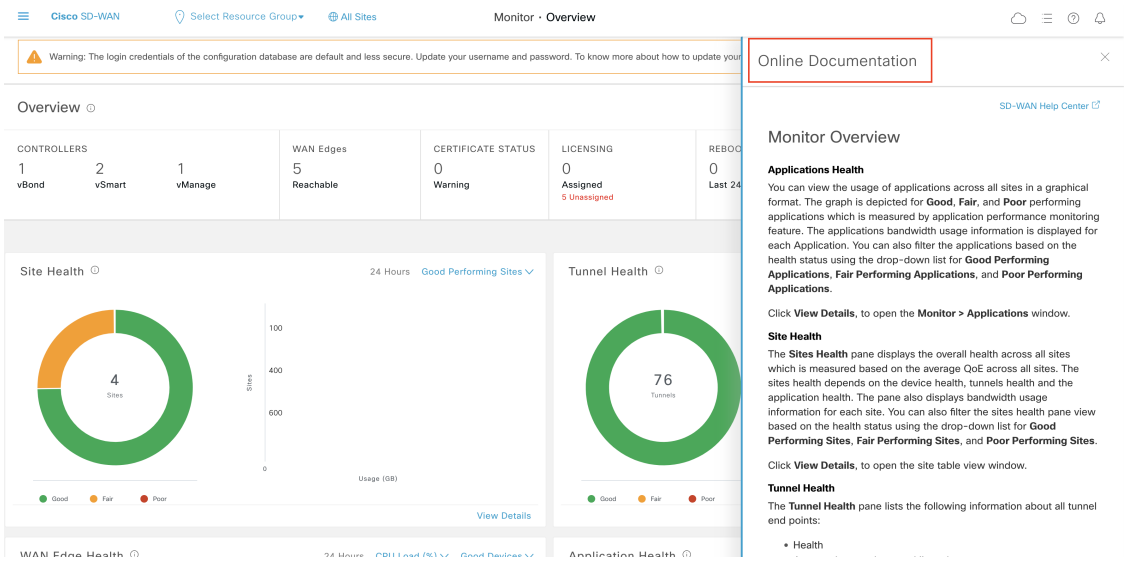


Cisco DNA Sense

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 Cisco IOS XE Routers
- Software Installation and Upgrade for vEdge Routers

- Field Notices
- Recommended Releases
- Security Advisories
- Cisco Bulletins

Full Cisco Trademarks with Software License