Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.15.x

First Published: 2024-08-27

Last Modified: 2025-07-22

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 17.15.1a

These release notes accompany the Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, which provides Cisco Catalyst SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco Catalyst 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 20.15.x

What's New for Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

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 17.15.1a

Feature	Description
Cisco Catalyst SD-WAN Systems and Interfaces	
Layer 2 (L2) VPN Multihoming and Hub-and-Spoke Support	With this feature, you can configure Layer 2 VPN on multiple devices on the same site in an active/standby configuration. This feature also enables Layer 2 connections using an indirect path, such as a hub, for point-to-multipoint connections within the Cisco Catalyst SD-WAN fabric.
Configure EtherChannels using Configuration Groups	With this feature you can configure EtherChannels on service and transport side using configuration groups.

Feature	Description
Load Balancing for EtherChannels on Individual Port Channels	With this feature you can load balance EtherChannels for individual port channels on service and transport side using CLI templates.
Cisco Catalyst SD-WAN Routing	
BFD Troubleshooting for Cisco Catalyst SD-WAN Using Radioactive Tracing	This feature provides the ability to troubleshoot BFD protocols using radioactive (RA) tracing. RA tracing enables debug logs across various processes which participates and handles a particular BFD session.
Multicast Support for Hub and Spoke Topologies	This feature enables efficient distribution of one-to-many traffic for hub and spoke devices. The multicast routing protocols like, IPv4 Multicast, IGMPv3, PIM SSM, PIM ASM, Auto RP and Static RP distribute data to multiple recipients. Using multicast overlay protocols in hub and spoke topology, a source can send a single packet of data to a single multicast address, which is then distributed to an entire group of recipients.
Cisco Catalyst SD-WAN Policies	
Packet Duplication using Underlay Fragmentation	This feature uses adjacency MTU to combine with underlay fragmentation which allows the successful transmission of packets that exceed the MTU limitations by breaking them down into manageable fragments and ensuring their reliable delivery.
Remote Preferred Color in Data Policy	You can set a remote preferred color in the data policy to control traffic routing based on the SLA criteria. See for Configure Traffic Rules information.
Service Insertion for Equinix	With this feature, you can deploy Palo Alto Networks firewall on Equinix and attach a service chain to Equinix interconnect gateway from the **Workflow Library** in Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN Security	
Cisco Umbrella Scope Credentials	This feature provides the ability to define and configure a new single Cisco Umbrella credential for both Umbrella SIG and Umbrella DNS.
Enhanced SGACL Logging	This feature enhances the Security Group Access Control List (SGACL) logging capability by using High Speed Logging (HSL) for Cisco IOS XE Catalyst SD-WAN devices. SGACL logging through HSL provides a logging method for security events that is more efficient and capable of scaling, useful in network environments experiencing high volumes of traffic.
Zscaler Sub-locations	This feature supports configuration of one or more Zscaler sub-locations for a given location.

Feature	Description
Cisco Catalyst SD-WAN Firewall High Availability	By implementing High Availability (HA) in Cisco Catalyst SD-WAN, you can set up two Cisco IOS XE Catalyst SD-WAN devices in either active-active or active-standby configurations. When HA is enabled, features like the Zone Based Firewall (ZBF) and Network Address Translation (NAT) utilize this functionality to synchronize their states between the devices, whether in active-standby or active-active modes. In the event of a failure of the active device, the standby device seamlessly takes over operations without interrupting session flows, thus eliminating the need for reconnection.
Share Traffic Information with Cisco Security Service Edge	Cisco SD-WAN Manager shares VPN and security group tag (SGT) information with Cisco Security Service Edge (SSE). This is called context information. SSE applies different policies to traffic based on the context information of the traffic.
Cisco Catalyst SD-WAN Cloud OnRamp	
Cloud OnRamp for SaaS Workflow	Cisco SD-WAN Manager allows you to select specific SaaS applications and identify best performing paths for each of these SaaS applications using a fully-guided workflow.
Cisco Catalyst SD-WAN Monitor and Maintain	
Alarm Notifications Using WebHooks	Configure a WebHook URL in Cisco SD-WAN Manager to receive alarm notifications in Webex or Slack.
Connect to and troubleshoot Cisco Catalyst SD-WAN solution using Cisco RADKit	Use tools and Python modules from Cisco Remote Automation Development Kit (RADKit) to securely connect to remote terminals, WebUIs, or desktops. Using RADKit, a TAC engineer can request the required information during the troubleshooting process, from the various devices and services, in a secure and controlled way.
Generate an Admin-Tech File with Custom Commands	This feature enhances the output of the admin-tech file with additional command output information. With this feature, You can generate a customized admin-tech file with the required show command output details to help in troubleshooting. Custom admin-tech is independent of tech, core, and logs flag.
View Packet Duplication Information for Tunnels	This feature provides a single chart option in Cisco SD-WAN Manager for viewing packet duplication information for tunnels.
Cisco Catalyst SD-WAN NAT	
Application-Level Gateway (ALG) in Service-Side NAT	Use an application-level gateway (ALG) to interpret the application-layer protocol and perform service-side NAT translations for FTP protocol.
Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)	
Create Regions and Assign Controllers Workflow	Cisco SD-WAN Manager introduces a fully-guided workflow that allows you to create multiple regions within your Cisco Catalyst SD-WAN fabric and assign Cisco SD-WAN Controllers to them.

Feature	Description
Policy Groups	
Preferred Remote Color in AAR Policy	You can set a remote preferred color in the AAR policy to control traffic routing based on the SLA criteria.
Region Support for Topology	**Level** topology attribute is supported for custom topologies where you could choose between **Sites** and **Regions**. When you add rules to your topology, match conditions using the **Region** condition.
Regions Support for Policy Groups	Associate devices from a particular region or subregion while deploying policy groups.
Cisco Catalyst SD-WAN Configuration Groups	
Configuration Catalog	This feature introduces a catalog functionality which provides a collection of pre-defined intent based configurations and policies. The Cisco Catalyst SD-WAN Portal hosts the catalog service, which is managed by Cisco. The Cisco SD-WAN Manager can download the readily available, cloud-hosted catalog entries from the Cisco Catalyst SD-WAN Portal and customize them as needed before deploying the configuration objects from the catalog entry onto devices in their network.
Create a Configuration Group Without Using a Workflow	This feature introduces a method for creating configuration groups directly on the **Configuration Groups** page of Cisco SD-WAN Manager without launching a workflow. After selecting a product solution, you can create a configuration group based on the available profiles for that solution. Cisco SD-WAN Manager creates the configuration group with the required profiles, which you can configure based on your requirement. This feature allows you to reuse previously created profiles. You can create, manage, and deploy the configuration group from one page.
Support for Specifying Default Values for Device Specific Variables of a Feature	You can provide a default value along with description to feature parameters when you select the **Device Specific** scope. Cisco SD-WAN Manager applies the default value of the parameter to the device while deploying the configuration group.
Cisco Catalyst SD-WAN Network-Wide Path Insight User	
Visibility into IPsec Drops	This feature provides enhancements to the Network-Wide Path Insight feature to provide granular visibility into the IPsec drops.
Cisco Managed Cellular Activation	
Managed Cellular Activation support for the IoT platforms and modules	The Managed Cellular Activation solution is supported in the IoT platforms and modules.
Cisco Catalyst SD-WAN Rugged Series Router Configuration Guide	

Feature	Description
Configure GNSS on PIMs Using Cisco SD-WAN Manager	This feature allows you to configure and manage the GNSS (Global Navigation Satellite System) PIM module on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager.
Deploying Smart Licensing Using Policy in Cisco Catalyst SD-WAN	
Workflow for Assigning Licenses to Devices	Introduced the License Assignment Workflow for assigning licenses to devices.
Cisco Catalyst SD-WAN Integrations	
Cisco Cyber Vision Integration	Cisco SD-WAN Manager supports integration with the Cisco Cyber Vision network security solution. You can configure devices in the network to monitor and inspect traffic on one or more interfaces and send traffic metadata or a copy of your network traffic to Cisco Cyber Vision Center to analyze it for security concerns.

Table 2: Cloud-delivered Cisco Catalyst SD-WAN

Field	Description
Interconnect Between Cisco Catalyst SD-WAN and Cisco Meraki SD-WAN	Cisco SD-WAN Interconnects is an automated workflow which enables administrators to easily configure, deploy, and monitor an interconnect between Cisco Catalyst SD-WAN and Cisco Meraki SD-WAN topologies using the Cisco Meraki dashboard. You can monitor IPsec tunnel status, eBGP session status, and VPN tunnel statistics from the Interconnects page on the Cisco Meraki dashboard.

Table 3: Cisco Catalyst SD-WAN Manager Release 17.15.2

Feature	Description
Cisco Catalyst SD-WAN Getting Started	
RSA Key Length Increase in Cisco SD-WAN Manager	Introduces 4096-bit RSA key support for certificate signing requests (CSR) for enterprise certificates.
Cisco Catalyst SD-WAN Policy Groups	

Feature	Description
Enhancements to Security Policy Using Policy Groups	The following enhancements are introduced with this release: • **Embedded Security** is called **NGFW** in Cisco SD-WAN Manager. • Create copies of security policy and sub-policy. • View all configured rules for specific policies in the **NGFW** policy dashboard. • For each rule, **Clone rule**, **Add rule on top**, and **Add rule below** options are added.

New and Enhanced Hardware Features

New Features

- Support for Cisco Managed Cellular Activation (eSIM): The Managed Cellular Activation solution provides a programmable subscriber identity module (SIM), called an eSIM, a physical SIM card that you can configure with a cellular service plan of your choice. Managed Cellular Activation is available for 5G Sub-6 GHz Pluggable Interface Module (PIM), model P-5GS6-GL, and for the Cisco Catalyst Wireless Gateway 113-4GW6.

  The solution also provides you a "bootstrap" cellular plan with limited data for connecting your device to the internet on Day 0. You need to set up your cellular plan details in Cisco SD-WAN Manager before you power on and onboard the device. This way, you can avoid using up the bootstrap data before your onboarding is completed.

  For information about configuring Cisco SD-WAN Manager with the details of your cellular plan in preparation for onboarding the device, see the Cisco Managed Cellular Activation Configuration Guide.

Note In this context, eSIM refers to a removable SIM pre-installed by Cisco. In other contexts, eSIM can refer to a non-removable SIM embedded in a cellular-enabled device.

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

Table 4: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

Behavior Change	Description
Updated the **show platform software ipsec fp active flow** command output.	The output of the **show platform software ipsec fp active flow** has been modified. The flow ID now supports a range between 0 - 4294967295. See the show platform software ipsec fp active flow command.
Updated the SLA class threshold values.	See the SLA Classes section, which describes the new SLA class threshold values.

Behavior Change	Description
Updated the **request platform software sdwanadmin-tech** command with supported options.	See the request platform software sdwan admin-tech command.
Updated the Policy Object Profile section with the new behavior on pagination when there are more than 50 profiles.	See the Policy Object Profile section.
Updated the size limit of the organization name to the range 1 to 128 for the organization-name command and the size limit of the interface name to the range 1 to 31 for the interface command.	See the sp-organization-name (system) and interface sections.
Updated the Configure Device Values section with the change in configuration groups for rollback timer. Only the Cellular Gateway solution in the configuration groups supports the rollback timer.	See the Configure Device Values section.
Updated the View Cflowd Information section for the show sdwan app-fwd cflowd commands to include support for up to 4000 flow records for each monitor (IPv4 and IPv6) from the cflowd database.	See the View Cflowd Information section.
Updated the Configure BFD for Routing Protocols section to include that the BFDs on the tunnel interface are inactive if sdwan mode is not configured for the tunnel interface.	See the Configure BFD for Routing Protocols section.
Information about provider and tenant remote servers and images on Cisco SD-WAN Manager.	See the Provider and Tenant Remote Servers and Images section.
Configuration of devices in SDCI cloud gateway extension using configuration groups is not supported.	See the Information About Configuring Devices for AWS Integration Using Configuration Groups section.
The policer increases the burst value when the user-configured value is lower than the calculated value, to prevent congestion and ensure optimal performance.	See the Policer Burst Tolerance section.
A static IP address is assigned by default if you assign a private color to a WAN interface while configuring a site using the configuration group workflow.	See the Overview of Configuration Group Workflows section.
Updated the **Response Code End** field in the Hunt Stop Rules table for consistency.	See the Server Group section.
In Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and earlier, click the **Send to Validator** button to send only the controller's serial number once to the Cisco Catalyst SD-WAN Validator.	See the Send the Controller Serial Numbers to Cisco Catalyst SD-WAN Validator section.

Table 5: Cisco IOS XE Catalyst SD-WAN Release 17.15.2

Behavior Change	Description
Mandatory Tenant ID and VPN ID with Prefix address for **show sdwan omp routes** command.	Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.1a, Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, and Cisco IOS XE Catalyst SD-WAN Release 17.15.2, the **show sdwan omp routes** command requires you to specify both the tenant ID and VPN ID when using a prefix address.

Important Notes, Known Behaviors, and Workarounds

Multi-Region Fabric

Cisco IOS XE Catalyst SD-WAN Release 17.15.x and Cisco Catalyst SD-WAN Control Components Release 20.15.x are the last releases to support these features:

- Secondary regions
- Subregions
- Management regions

From Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Control Components Release 20.15.1, configuration of these features is possible only by API.

Because later releases do not support these features, we advise you to update your network design and configuration to use alternative solutions where possible.

See End of support for three types of regions for further details.

Disaster Recovery

The user account used for disaster recovery supports only local authentication and does not support remote authentication methods such as TACACS+ or RADIUS. This user must be dedicated solely to disaster recovery tasks and must not be used for any other functions, such as cluster management because of the following reasons:

- Reliability: Using dedicated accounts for DR sync minimizes configuration errors and reduces operational risks.
- Resilience: Prevents issues related to user lockouts or account overrides, ensuring DR processes are not impacted by administrative changes to other accounts.
- Audit and compliance: Dedicated users provide clear separation for auditing purposes, making it easier to track and log DR-related activities.
- Industry standard: All our customers, including those in highly regulated sectors such as finance, follow this model. It is the recommended and supported deployment standard.
- Avoid remote authentication issues: TACACS-based users are prone to disruptions due to potential latency or connectivity issues with remote authentication servers. Using local accounts eliminates these risks, ensuring uninterrupted DR sync and cluster operations.

- Password rotation: Capabilities are provided via API/GUI on active cluster and through CLI on standby cluster.

TLOC extension configuration

If a device

- is using Cisco IOS XE Catalyst SD-WAN Release 17.9.x or earlier, and
- the device has a tunnel interface configuration includes a TLOC extension,

then you cannot upgrade to one of these:

- 17.12.1 through 17.12.4
- 17.15.1 through 17.15.2

Attempting such an upgrade causes the device to crash and enter a rollback state.

If you have a TLOC extension configured and need to perform such an upgrade, remove the TLOC extension configuration from the tunnel interface configuration before upgrading.

This issue was fixed and does not apply for upgrades from one of these releases:

- 17.12.5 and later releases of 17.12.x
- 17.15.3 and later releases of 17.15.x
- 17.18.1a and later

Resolved and Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.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 17.15.4

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.4

Identifier	Headline
CSCwo05703	VFR is not dynamically disabled after ZBFW removal on Cisco SD-WAN Manager
CSCwp01534	Elevated memory usage on ISR1100-4G/6G devices.
CSCwo22511	Cisco IOS XE Catalyst SD-WAN device: confd_cli high cpu utilization after executing "show omp tlocs"
CSCwm96744	After WAN failover IPsec tunnel takes 12+ hours to recover
CSCwn54491	BFD sessions don't come up after a reboot on a spoke with a dual-stack WAN (IPv4 and IPv6).
CSCwo50617	Reply unknown unicast packet with non-self MAC address on GRE tunnel
CSCwn53608	BFD Packet drops on ATM interface after upgrade

Identifier	Headline
CSCwo76207	Flow stickiness does not work when match based on app-family
CSCwm72414	Data Policy SIG action with CoR SaaS DIA path blackholes DNS traffic
CSCwn85877	Cisco IOS XE Catalyst SD-WAN device fragments the packets with interface MTU instead of tunnel PMTU
CSCwo01770	E-AAR Local Loss does not work on COFF Platforms.
CSCwo84428	Memory leak under vdaemon process with DTLS on SNMP polling on Cisco IOS XE Catalyst SD-WAN device
CSCwo92093	Clean up needed for /tmp files created post admin tech generation
CSCwo10491	IPV6 BFD session sourced from a loopback (unbind) is down due to BFD offload.
CSCwp24639	Device reload after vpn config changes on Cisco SD-WAN Manager
CSCwj49155	DNS Channel uses same source port in every connection
CSCwo58622	Cisco IOS XE Catalyst SD-WAN device Elixirwifi: native Vlan config is not load by config reset on WLAN Interface
CSCwk31324	Data Policy next-hop action with CoR SaaS DIA path blackholes traffic
CSCwo81270	Cisco IOS XE Catalyst SD-WAN device AMP allows malware files when downloading from the internet and FTP simultaneously
CSCwn69868	Unable to come up control connections with Cisco Catalyst SD-WAN Controllers after they are added and down/up
CSCwo98521	Memory leak in cxpd with HTTPs endpoint probing having more than 2 second RTT
CSCwo05158	SLA events not getting the correct values from the Cisco IOS XE Catalyst SD-WAN device
CSCwn42496	SDWAN-SIT: Encore crashed @bfd_send_and_detect_sleep_time during soak run
CSCwo78780	Critical process ompd fault on rp_0_0 restart happened with rc=134

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.4

Identifier	Headline
CSCwo66099	Cisco IOS XE Catalyst SD-WAN device service side BFD flaps
CSCwp20177	DHCP client identifier inconsistency on Cisco IOS XE Catalyst SD-WAN device
CSCwm37504	Cisco IOS XE Catalyst SD-WAN device Upgrade 17.3.3 to 17.9.5a removes OMP service side VRF address-family configuration
CSCwe19394	Cisco IOS XE Catalyst SD-WAN device may boot up into prev_packages.conf due to power outage

Identifier	Headline
CSCwo34471	Cisco SD-WAN Manager NAT timedout sessions are not removed
CSCwo42664	17.12 - keyman core files on Cisco IOS XE Catalyst SD-WAN device
CSCwo75657	Maximum control connection not equal to maximum omp sessions on Cisco IOS XE Catalyst SD-WAN device
CSCwp12196	Cisco IOS XE Catalyst SD-WAN device unexpectedly reloads due to memory corruption on a notification queue in FTMd
CSCwo11688	Continuous endpoint tracker log messages when DNS query fails in tracker-group

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.3a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.3a

Identifier	Headline
CSCwn53881	Rekeying fails for the PWK and Non-PWK interworking use case.
CSCwn49931	The FMAN_FP process crashes while running longevity traffic with triggers.
CSCwn45512	The router reaches the show ip nat translations total limit, even with a low number of active NAT table entries.
CSCwn34457	After a power cycle, logging into the router fails with the error "Authentication failed."
CSCwm13277	The Catalyst 8000v device experiences a crb_linux_iosd_vxe crash after rebooting with telemetry configurations.
CSCwn54491	BFD sessions fail to come up after a reboot on a spoke device with a dual-stack WAN (IPv4 and IPv6).
CSCwn40906	A router crash is observed when optimizing encrypted traffic using DRE.
CSCwo08234	The Zscaler SSE tunnel is incorrectly established using TLOC extension after a router reload.
CSCwn52348	Removing and re-adding NAT intermittently causes BFD to go down.
CSCwm50619	A data policy commit failure occurs when export-spread is enabled in the Cflowd configuration.
CSCwn12971	Certain OMP routes return the error "% No such element exists" if the prefix length is not specified.
CSCwn86439	TCP flows using segment routing fail to set the MSS when passing through sdwan_l2.
CSCwm48459	Software crash with Critical process vip_confd_startup_sh fault on rp_0_0 (rc=6)
CSCwn35075	Cisco IOS XE Catalyst SD-WAN device: An unexpected reload occurs after an Overlay Session is deleted during the deletion of the AVL tree.

Identifier	Headline
CSCwn93052	The static default route fails to install in the routing table due to an issue with the track-default-gateway feature.
CSCwo21215	In version 17.12.4 Respin, BFD goes down with private color behind NAT for carrier7 and carrier8.
CSCwm72748	The OMPd process crashes with a Sig-abort error when the pthread limit is reached .
CSCwn39963	NAT DIA packets randomly dropped due to Ipv4RoutingErr
CSCwn39940	Crash seen with Enhanced Application-Aware Routing feature (additional code changes for CSCwn16182)
CSCwo32083	The default route was lost after moving from physical interface to sub-interface case.
CSCwn65833	Unexpected reload on Cisco IOS XE Catalyst SD-WAN device due to NWPI trace elephant flow.
CSCwn43979	Catalyst 8500L: Overruns caused by Extended AR window feature.
CSCwn16182	Crash seen shortly after Enhanced Application-Aware Routing is enabled.
CSCwm61790	SDWAN BFD does not start bfd detection timer on BFD_INIT state.

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.3a

Identifier	Headline
CSCwn85877	Cisco IOS XE Catalyst SD-WAN device fragments the packets with interface MTU instead of tunnel PMTU.
CSCwj49155	DNS Channel uses same source port in every connection.
CSCwm37504	vManaged Cisco IOS XE Catalyst SD-WAN device Upgrade from 17.3.3 to 17.9.5a removes OMP service side VRF address-family configuration.
CSCwe19394	Cisco IOS XE Catalyst SD-WAN device: device may boot up into prev_packages.conf due to power outage.
CSCwo34471	SDWAN NAT timedout sessions are not removed.
CSCwo42664	17.12 - keyman core files on Cisco IOS XE Catalyst SD-WAN device
CSCwn51404	A crash occurs in the critical process ftmd because the parent TLOC delete happens before the child TLOC add.
CSCwo42502	ISR1100-4G Cisco IOS XE Catalyst SD-WAN device routers have the process "cpp_sp_svr" as the top memory consumer.
CSCwn12847	IPSec umbrella tunnels are going down everytime an umbrella side executes the rekey.

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.2a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.2a

Identifier	Headline
CSCwk28794	SNMP returns incorrect value for the interface when using switchport.
CSCwk39391	Multicast drops seen due to IpsecOutput drops - OUT_IPV4_SA_NOT_FOUND.
CSCwk75733	Custom Applications may not be programmed properly.
CSCwk69490	Crash when mistakenly running incomplete command show sdwan app-route stats local-color.
CSCwk70415	IOS-XE stuck thread unexpected reload with NAT BPA configuration.
CSCwk31804	Cisco SD-WAN Manager Control Connection does not come up with local dialer when remote-Cisco IOS XE Catalyst SD-WAN device uplink is down.
CSCwm05718	CXPD crashes on upgrade from 17.12 to 17.15 with 'probe-path trigger' configured.
CSCwm07994	Unexpected reload on IOS-XE because encrypted IPSEC packet buffer got into the decryption queue.
CSCwm07564	Cisco IOS XE Catalyst SD-WAN device: Data-policy local-tloc-list breaks RTP media stream.
CSCwm02632	Configuring route-aggregate from Cisco SD-WAN Manager without 'aggregate-only' looks misleading.
CSCwk87944	VRRP switchover with TLOC preference change is generating rekey and crypto add/delete events.
CSCwm27495	OMP route is being advertised although the route is not available (network statement + NAT DIA VPN).
CSCwm28775	Certificate (ios_core.p7b bundle) update required for umbrella DNS for TOKEN method on 17.6/.9/.12
CSCwf62943	Cisco IOS XE Catalyst SD-WAN device: System image file is not set to packages.conf when image expansion fails due to disk space.

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.2a

Identifier	Headline
CSCwn53881	Rekey doesn't work for PWK and non-PWK interworking usecase.
CSCwf51721	Enterprise certificate status displayed as "Not Applicable" post rollback from viptela to ios-xe.
CSCwn93052	Static default route not getting installed in routing table due to issue with track-default-gateway.

Identifier	Headline
CSCwn34457	Post power cycle, unable to login to router due to error authentication failed.
CSCwn52348	Remove and re-add NAT causes BFD to go down (Intermittent).
CSCwn49931	FMAN_FP crash running longevity traffic with triggers.
CSCvu18068	Cisco IOS XE Catalyst SD-WAN device umbrella integration.
CSCwm13277	SIT: crb_linux_iosd_vxe crash in C8000v device after rebooting with telemetry configuration.
CSCwm48459	Software crash with Critical process vip_confd_startup_sh fault on rp_0_0 (rc=6).
CSCwm50619	Data policy commit failure occurs when export-spread is enabled in Cflowd configuration.
CSCwn51404	Crash due to Critical process ftmd, parent TLOC delete is happening before child TLOC add.
CSCwm72748	The OMPd process crashes with a SIGABORT error when it hits the pthread limit.
CSCwn12847	IPSec umbrella tunnels are going down everytime umbrella side executes the rekey.
CSCwn45328	Unable to create unified policy with IPv6 rule when any other rule has AIP with TLS action decrypt.
CSCwm72414	Data Policy SIG action with CoR SaaS DIA path blackholes DNS traffic.
CSCwn82653	Memory high and the device crashed due to OMPD.
CSCwn65833	Unexpected reload on Cisco IOS XE Catalyst SD-WAN device due to NWPI trace elephant flow.

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

Identifier	Headline
CSCwj83844	Cisco Catalyst IR1101 Rugged Series Router: Default queue size is too low for configure QoS bandwidth.
CSCwj51700	CPP crashes after re-/configuring "ip nat settings pap limit ... bpa" feature in high QFP state.
CSCwk03686	Crash due a segmentation fault due a negative value.
CSCwk42634	%PMAN-0-PROCFAILCRIT: R0/0: pvp: A critical process vip_confd_startup_sh has failed (rc 6)
CSCwj53456	Crash triggered by 'crypto ikev2 cluster detail' command.

Identifier	Headline
CSCwk26247	Catalyst 8500L Edge Platform QFP stuck threads crash while handling netflow features under Autonomous mode.
CSCwk33173	EzPM application-performance profile cause memory leak and crash with long-lived idle TCP flows.
CSCwk16333	Cisco IOS XE Catalyst SD-WAN device repeatedly crashes in FTMd due to FNF Flow Add.
CSCwj95633	SDWAN: SAIE Application - No Data to Display over Cisco SD-WAN Manager for IOS XE router.
CSCwk42190	Configuration and dp show command don’t match the dp oper output.
CSCwj06950	Cisco 1000 Series Integrated Services Routers - DSL module gets stuck in a booting state.
CSCwj96852	Return traffic for Outside to Inside NAT traffic received on one TLOC is forwarded out of other TLOC.
CSCwk39131	Cisco IOS XE Catalyst SD-WAN device crashed when issuing "show sdwan ftm next-hop chain all"
CSCwk37351	IOS XE Router: Unexpected Reboot during PVDM OIR.
CSCwk22225	FTMd crashes after receiving credentials feature template update from Cisco SD-WAN Manager.
CSCwj48909	17.14 Coredump observed in tracker module while running cxp_sig_auto_tunnel suite.
CSCwk23723	Cisco 1000 Series Integrated Services Routers/Cisco Catalyst Series 8200/8300/8500L : Mean queue calculation is incorrect on WRED hierarchical QoS.
CSCwj31476	Cisco IOS XE Catalyst SD-WAN Release 17.14.x/ 20.14: DSL device feature template suite fails with CONFD ERROR 'no switchport access vlan 4'
CSCwk45165	The fman_fp Memory Leak on Catalyst 8500L Edge Platform.
CSCwj16153	C8300-2N2S-4T2X: 10G front-panel port do not go down on single mode fiber when Rx side goes down.
CSCwj76501	Catalyst 8500L Edge Platform - Data Plane Crash in ERSPAN Processing
CSCwj84949	Unencrypted traffic due to non-functional IPsec tunnel in FLEXVPN hub & spoke setup.
CSCwi56641	100G/40G: QSFP fiber: C9500X-28C8D reports link-flap error when peer C8500-20X6C reloads.
CSCwk20583	C8500-12x4QC: 40G interfaces with breakout configurations flap after reload.
CSCwj90614	High CPU utilisation for confd_cli.

Identifier	Headline
CSCwi81026	SDWAN BFD sessions flapping during IPSec rekey in scaled environment.
CSCwk39268	[2.3.7.x] sdn-network-infra-iwan failing to renew with "hash sha256" > 17.11
CSCwj76662	Cisco IOS XE Catalyst SD-WAN device- High memory utilization due to "ftmd" process.
CSCwj92560	STCAPP command removed from VG410 after reload.
CSCwk31715	After deleting a NAT configuration, the IP address still shows up in routing table.
CSCwk42253	Unexpected reboot when a HTTP connection failed with 404 on a controller mode router.
CSCwj42448	APN password in plain text when cellular controller profile is configured.
CSCwk12524	Device reloaded due to ezManage mobile app Service.
CSCwk53680	[vg400] Inbound calls through VG400 results in phantom calls (64.3.0, 60.1.4, 62.3.3)
CSCwk44078	GETVPN / Migrating to new KEK RSA key doesn't trigger GM re-registration.
CSCwj23674	Dialer interface MAX MTU for PPPOA is 1492.
CSCwk22942	Unable to build two IPSec SAs w/same source/destination where one peer is PAT'd through the other.
CSCwj96092	20/17.14: ICMP tracker type (from echo to timestamp) change causes tracker to fail.
CSCwj99827	Cisco IOS XE Catalyst SD-WAN device unexpectedly reloads due to a crash in 'vdaemon' process.
CSCwi99454	cEdgeFNF test_tunnel_name_change_CSCvt57024 case failed due to session of pm5 was not alive
CSCwj02401	Cisco IOS XE Catalyst SD-WAN device: Router reloaded when generating admin tech while processing very high number of flows.
CSCwj40223	The appRouteStatisticsTable sequence misordered in CISCO-SDWAN-APP-ROUTE-MIB or OS returns wrong order.
CSCwk19725	The add FNF cache limit for show sdwan app-fwd flows for CSCwj02401.
CSCwk22312	C8500-12X & C8500-12X4QC: Input errors and overrun on Port Channel interface and physical interface.
CSCwk56504	In NAT64 scenario, IPv4 packets that needs translation might be dropped by Cisco ASR 1000 Series routers.
CSCwj86794	Cisco ASR 1000 Series routers crashes while processing an NWPI trace.
CSCwe52258	VG420 needs to keep startup vty lines configuration after pulling config from WxC.

Identifier	Headline
CSCwj67591	20.14:SD-Routing Brownfield - chassis activate effective only after second re-try - with new uuid.
CSCwj54638	ASR1001-HX: EVC Q-in-Q configuration may filter out certain vlans.
CSCwj32347	DIA Endpoint tracker not working with ECMP routes.

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.15.1a

Identifier	Headline
CSCwi76516	The Managed Cellular Activation solution configuration tamplate deployemt fails.
CSCwk95308	CRC errors increment on down interface of Catalyst 8500-12X.
CSCwk75733	Custom Applications may not be programmed properly.
CSCwk89256	Cisco SD-WAN Manager/IOS-XE 17.9.3 speed mismatch in IOS-XE configuration after device template push for ISR.
CSCwm07994	Router crash with stuck threads.
CSCwk85704	The sd-routing:"match traffic-category " through Cisco SD-WAN Manager add-on CLI push failed.
CSCwm07396	ASR1K/C8500-12X* and C8500-20X6C :Few BFD sessions down after clear mka session on client.
CSCwm07651	ISR4K crash due to dbgd process.
CSCwm11819	Cisco ASR 1000 Series routers crash due to SIGSEGV | fman_fp_image fault on fp_0_0 (rc=139)
CSCwj01917	After Upgrade to 17.9.4a, Cellular Interface IP ADDRESS NEGOTIATED is mismatching.
CSCwk87944	VRRP switchover with tloc preference change is generating rekey and crypto add/delete events .
CSCwk98006	Unable to Establish NAT Translations with ZBFW enabled.
CSCwk28794	SNMP returns incorrect value for the interface when using switchport.
CSCwj76689	Cisco Catalyst 8000V Edge Software configuration lost after .bin upgrade from 17.12.1 to 17.14.1
CSCwk86355	File transfer fails from Cisco SD-WAN Manager 20.9.5 /home/admin to Cisco IOS XE Catalyst SD-WAN device 17.6.5 bootflash: "lost connection"
CSCwk49806	ASR1002-HX router running IOS 17.06.05 rebooted unexpectedly due to process NHRP crash.
CSCwk81360	Cisco IOS-XE Router can reboot unexpectedly while configuring NAT static translation.

Identifier	Headline
CSCwk62954	Multiple "match address local interface <int>" not pushed from Cisco SD-WAN Manager under crypto profile.
CSCwk63722	Startup configuration failure post PKI server enablement.
CSCwk97092	17.15:MKA session not coming up after shut/no shut with EVC.
CSCwm07564	Cisco IOS XE Catalyst SD-WAN device: data-policy local-tloc-list breaks RTP media stream.
CSCwk25731	[HCA] C8500-20X6C flaps more than once when interface is bounced with SRBD optics connected to N7706.
CSCwk54544	SD-WAN ZBFW TCAM misprogramming after rules are reordered on Cisco Catalyst 8300 Series Edge Platforms.
CSCwk89523	Cisco Catalyst 8500 Series Edge Platforms, IOSd crash during function to add/delete a MAC address from the MAC accounting table.
CSCwk74298	Cisco IOS XE Catalyst SD-WAN device denied for template push and some show commands with error application communication failure.
CSCwk86062	LTE NIM-EM7455, Modem locks up after reboot of router, modem reset or cellular profile change.
CSCwk98578	Cisco Catalyst 8500 Series Edge Platforms/ XE 17 / GETVPN ipv6 crypto map not shown in interface configuration.
CSCwj42448	APN password in plain text when Cellular controller profile is configured.
CSCwj05500	Cisco Catalyst 8000V Edge Software - Accelerated Networking stops working due to driver issue.
CSCwk70630	9800-L 17.12.02 Cannot import device certificate.
CSCwk69597	Cisco Catalyst 8000V Edge Software running config write memory did not persist after reload.
CSCwk97930	Crash occurs when IPv6 packets with link-local source are forwarded to SDWAN tunnels.
CSCwm13223	IOS-XE 17 Crashes in IOSd Due to Malformed DMVPN-5-NHRP_RES_REPLY_IGNORE Syslog.
CSCwk79454	Endpoint Tracker does not fail if default route is removed.
CSCwi40697	Modem may not come back up from FW upgrade with LM960A18 and FN980 modems.
CSCwk52677	C1118-8P / DSL router crashing due to %PLATFORM-3-ELEMENT_CRITICAL memory level / iomd process.
CSCwk90014	NAT DIA traffic getting dropped due to port allocation failure.

Identifier	Headline
CSCwi87546	Cisco 4000 Family Integrated Services Router Unexpectedly reboot due to QFP CPP stuck at waiting for rw_lock - Lock id of 0 released.
CSCwk61238	RRI static not populating route after reload if stateful IPSec is configured.
CSCwk72795	Cisco ASR 1000 Series routers no statistics for the SBFD protocol.
CSCwk95044	17.12.03.CSCwj42249.SPA.smu.bin drops when Packet Duplication link fails-over.
CSCwj87028	The cflowd showing custom APP as "unknown" for egress traffic when using DRE Opt.
CSCwm11348	Enpoint Tracker reporting error due to "DNS Querry Error".
CSCwk20995	PPPoE session with sub-interface getting stuck after reboot.
CSCwk89330	Cisco IOS XE Catalyst SD-WAN device is dropping data plane packets, while bfd sessions are up.
CSCwm08545	Centralized Policy Policer worked per PC on the same site not per site/vpn-list.
CSCwk34187	cEdge_Nbar: application Dicom under family Middleware not displayed in DPI flows and Cisco SD-WAN Manager.
CSCwm01269	Cisco SD-WAN Manager speed test on Cisco Catalyst 8300 Series Edge Platforms is giving better result from TLOC extension from the secondary router.
CSCwf62943	Cisco IOS XE Catalyst SD-WAN device: System image file is not set to packages.conf when image expansion fails due to disk space.
CSCwm00309	Packets not hitting the correct data policy after modifying the action of a sequence.

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.

AI Assistant on Cisco SD-WAN Manager

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.15.1

On Cisco SD-WAN Manager, click Cisco AI Assistant. The AI assistant is available only to cloud customers. You can use this feature for the following use cases:

- Product and Features: Provides information about Cisco Catalyst SD-WAN and the features introduced in this release.
- Monitor Network: Provides information about the network and application health.

To enable the AI assistant feature:

1. Enable cloud services in **Administration** > **Settings**.
2. Enter the **Smart Account Credentials** and click **Save**.

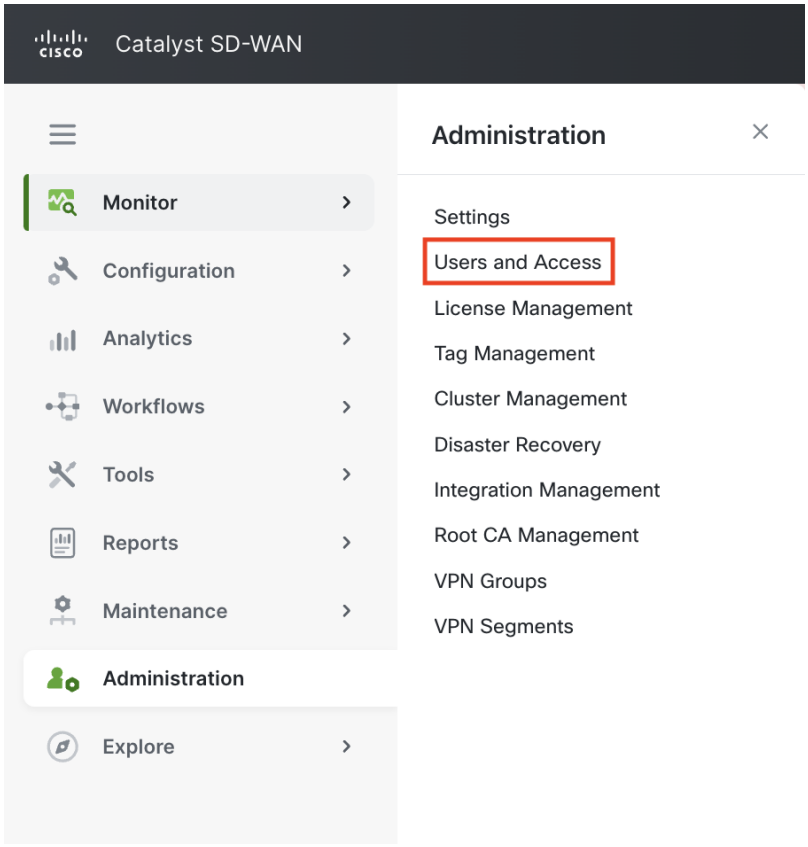
Cisco Catalyst SD-WAN Manager GUI Changes

This section presents a summary of the significant GUI changes between Cisco Catalyst SD-WAN Manager Release 20.14.1 and Cisco Catalyst SD-WAN Manager Release 20.15.1.

- Administration menu, Users and Access

  In the **Administration** menu, the **Manage Users** menu is renamed to **Users and Access**.

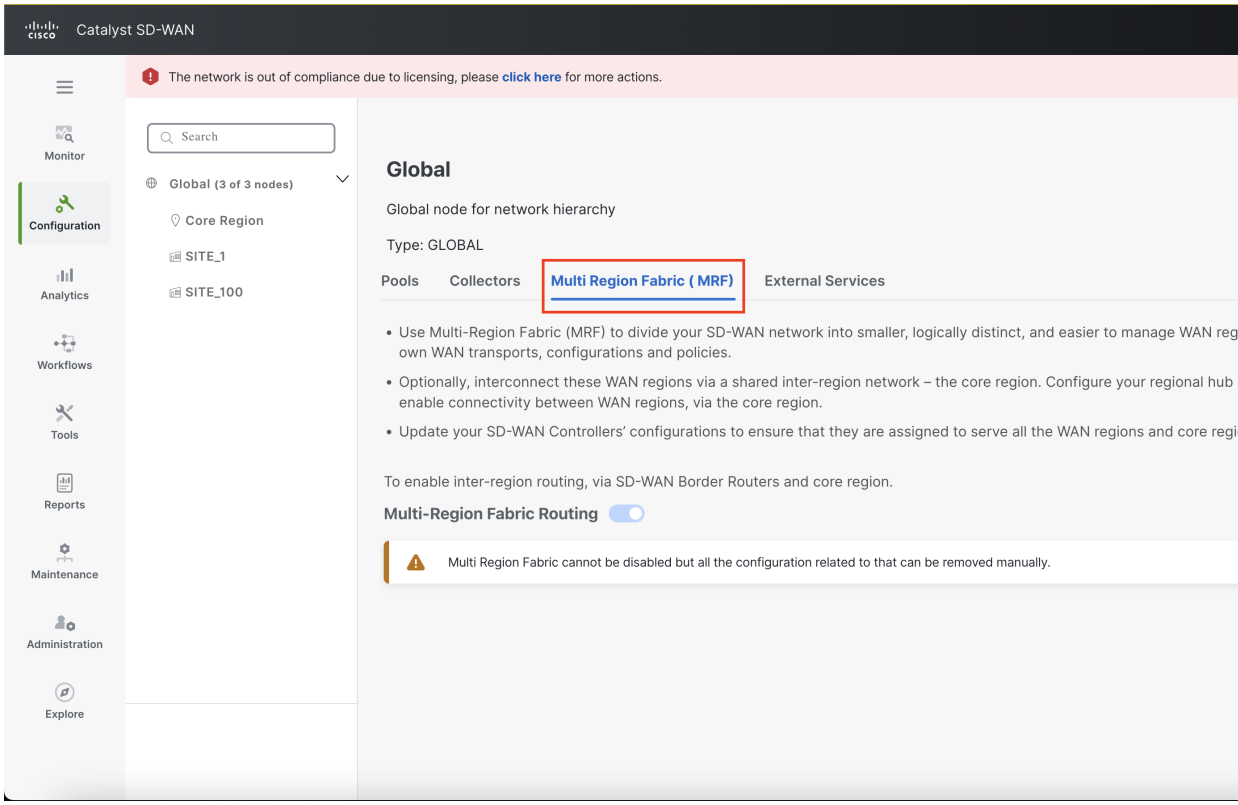
  Figure 1: Administration Menu



- Network Hierarchy page, Multi Region Fabric (MRF) tab

  On the **Configuration** > **Network Hierarchy** page, the **Network Settings** tab is renamed to **Multi Region Fabric (MRF)**.

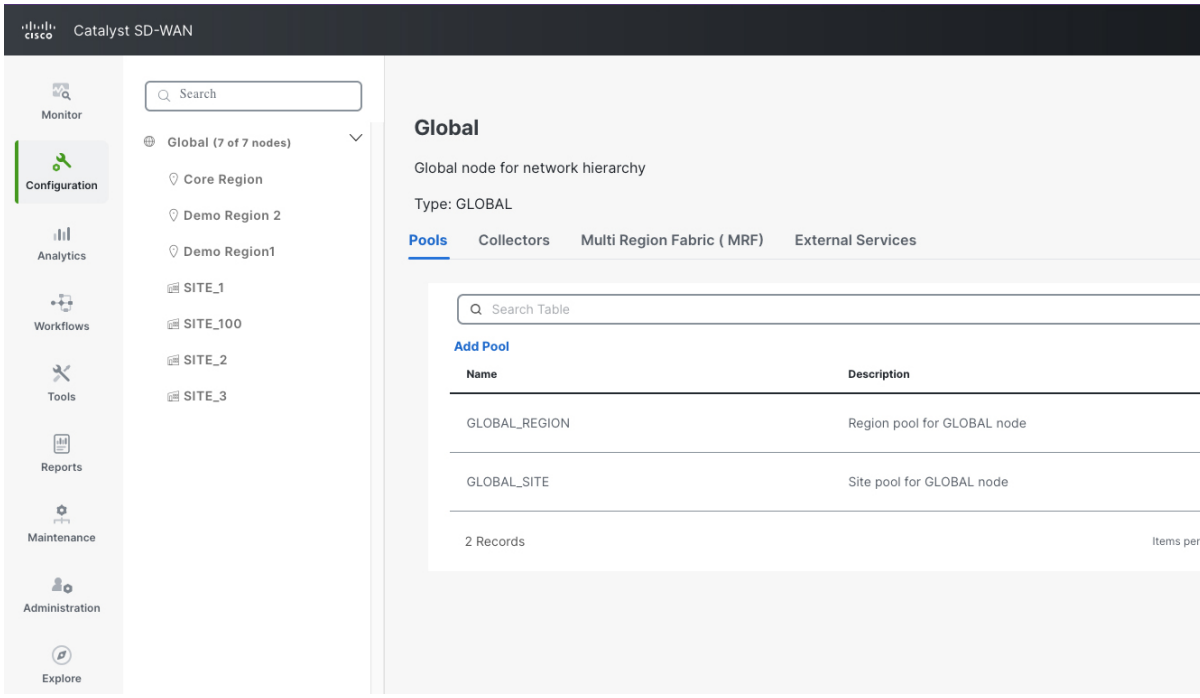
Figure 2: Network Hierarchy Page, Multi Region Fabric (MRF) Tab



- Secondary regions and subregions

  On the **Configuration** > **Network Hierarchy** page, it is no longer possible to create secondary regions or subregions. From this release, these are supported only through API.

Figure 3: Network Hierarchy Page



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
- Cisco Recommended Catalyst SD-WAN Software Versions for Controllers and WAN Edge Routers

Full Cisco Trademarks with Software License

SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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