Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.9.x

First Published: 2022-08-26

Last Modified: 2024-02-20

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 17.9.1a

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 17.9.1a, 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 vEdge Devices, refer to Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.9.x.

For release information about Cisco Catalyst SD-WAN Control Components, refer to Release Notes for Cisco Catalyst SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.9.x

What's New for Cisco IOS XE Catalyst SD-WAN Release 17.9.x

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.

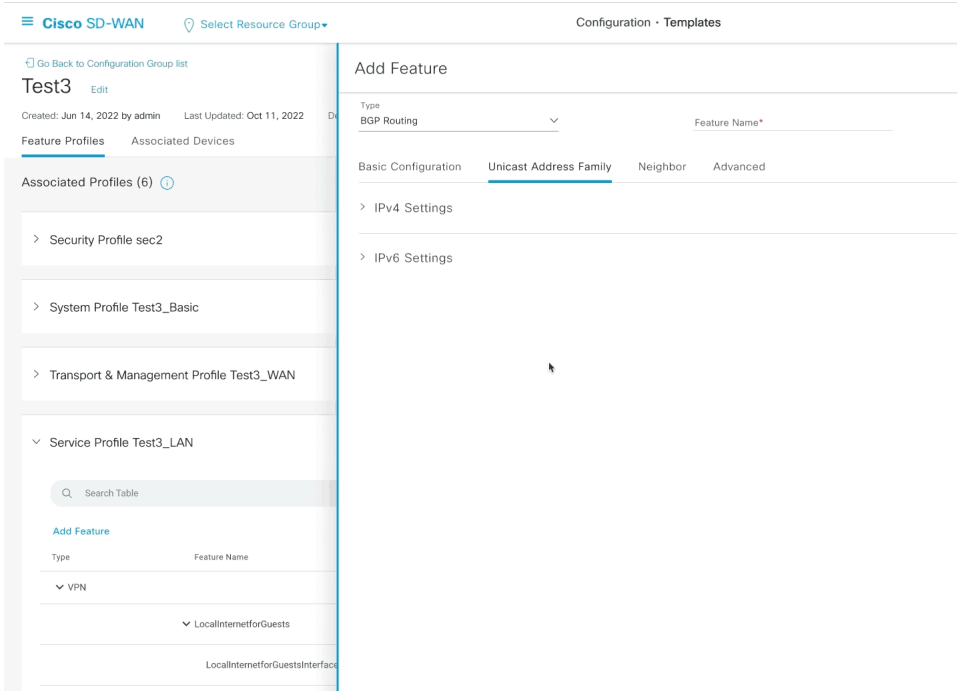
Table 1: Cisco IOS XE Catalyst SD-WAN Release 17.9.4

Feature	Description
Cisco Catalyst SD-WAN Analytics	
Easy Onboarding of Cisco SD-WAN Analytics into Cisco Catalyst SD-WAN Manager	This feature enables you to easily onboard Cisco SD-WAN Analytics into Cisco Catalyst SD-WAN Manager.

Table 2: Cisco IOS XE Catalyst SD-WAN Release 17.9.2a

Feature	Description
Cisco Catalyst SD-WAN Systems and Interfaces	

Feature	Description
Changes in the **Add Feature** and **Edit Feature** Forms	

Feature	Description
	The following enhancements are introduced in the **Add Feature** and **Edit Feature** forms. • Accordion menus have been introduced to reduce scrolling. Click an accordion or the corresponding header to show or hide the content associated with it.  • A common template has been introduced to present repeated data.

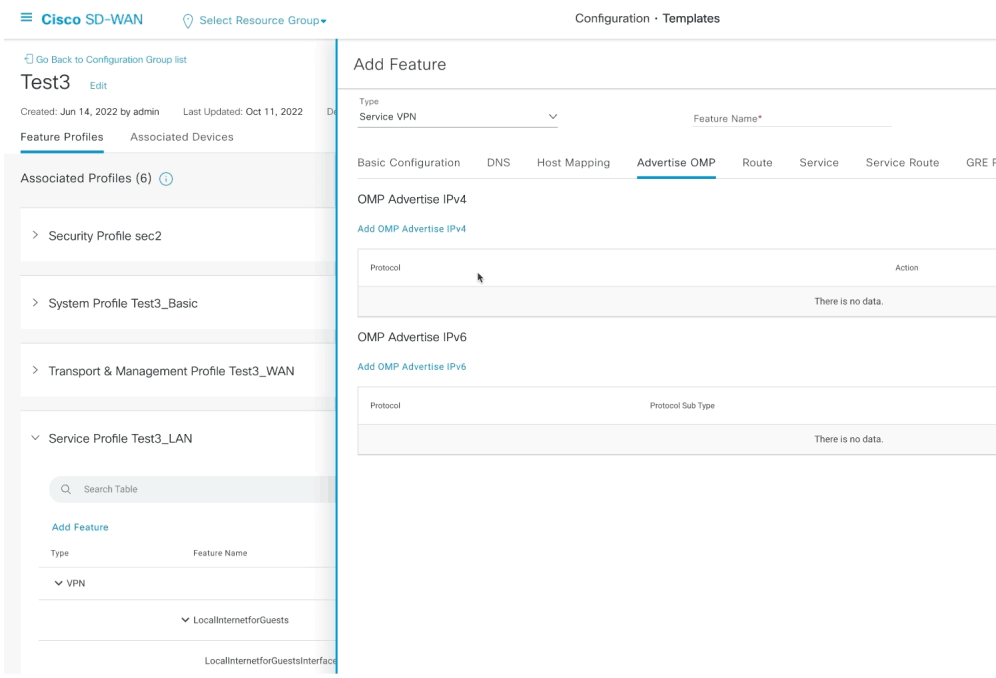
Feature	Description
	
Cisco Catalyst SD-WAN Monitor and Maintain	
Device Information	The **Monitor > Devices** page displays the devices that are newly added or synced to Cisco SD-WAN Manager using the options available on the **Configuration > Devices** page.
Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)	
Migrate a BGP-Based Hierarchical Core Network to Multi-Region Fabric	This feature facilitates migrating a BGP-based hierarchical core network into a Cisco Catalyst SD-WAN Multi-Region Fabric-based topology by alleviating the need of complex control policy definitions and the existence of a BGP core.
Cisco Catalyst SD-WAN Getting Started Guide	
Manage HSEC Licenses	This feature enables you to install high security (HSEC) licenses on devices managed by Cisco SD-WAN Manager. An HSEC license is required to enable devices to support encrypted traffic throughput of 250 Mbps or higher.

Table 3: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started	

Feature	Description
Support for License Management Using a Proxy Server	If you configure Cisco SD-WAN Manager to use a proxy server for internet access, Cisco SD-WAN Manager uses the proxy server to connect to Cisco SSM or an on-premises SSM.
Support for Managing Licenses Using Cisco Smart Software Manager On-Prem	Cisco SD-WAN Manager supports management of device licenses, using a Cisco SSM On-Prem license server. This is useful for organizations that use Cisco SSM On-Prem to accommodate a strict security policy that does not permit devices to communicate with Cisco SSM over a direct internet connection.
Renew Device CSR	This feature allows you to reset the RSA private and public keys, and generate a CSR that uses a new key pair. In earlier releases, the generation of CSR used the existing key pair.
Support for Software Maintenance Upgrade Package	This feature enables support for Software Maintenance Upgrade (SMU) package that can be installed on Cisco IOS XE Catalyst SD-WAN devices. The SMU package provides a patch fix or a security resolution to a released Cisco IOS XE image. Developers can build this package that provides a fix for a reported issue without waiting to make the fix available in the next release.
Cisco Catalyst SD-WAN Systems and Interfaces	
Hardened Passwords	This feature lets you configure Cisco SD-WAN Manager to enforce predefined medium-security or high-security password criteria.

Feature	Description

Configuration Groups and Feature Profiles (Phase II)	The following enhancements are introduced for the Configuration Group feature.
	• Adds support for the following features:
	  • SNMP
	  • Cellular Interface
	  • BGP Routing (transport and management profile)
	  • Wireless LAN
	  • Switch Port
	  • SVI Interface
	  • DHCP Server
	  • ThousandEyes
	• Adds the IPv6 configuration support in the VPN, interface, and BGP features.
	• Adds the following options to the Global settings, which are a part of the system profile. These options have been added to the **Other Settings** tab.
	  • Generate keepalive timers when incoming or outgoing network connections are idle
	  • Enable small TCP and UDP servers
	  • Enable console logging
	  • Enable IP source routing
	  • Display log messages to a vty session
	  • Enable SNMP IFINDEX persistence
	  • Enable BOOTP server

Create Configuration Group Workflow for a Single-Router Site	This feature introduces the Create Configuration Group workflow. The simplified workflow consolidates the various settings pages into a single page so that you can easily review your configuration at once. It also enables you to set up the WAN and LAN routing, in addition to the basic settings, at the time of creating a configuration group. As a result, any configuration created from the workflow is now immediately deployable.
Network Hierarchy and Resource Management	This feature enables you to create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. The network hierarchy and the associated resource IDs, including region IDs and site IDs, help you apply configuration settings to a device. In addition, the introduction of the resource manager in Cisco SD-WAN Manager automatically manages these resource IDs, thereby simplifying the overall user experience of Cisco Catalyst SD-WAN. You can create a region only if you enable the **Multi-Region Fabric** option in Cisco SD-WAN Manager.

Feature	Description
Wireless Management on Cisco 1000 Series Integrated Services Routers supporting WIFI6 WLAN module	This feature enables you to configure the wireless LAN settings on WiFi6-capable Cisco 1000 Series Integrated Services Routers using Cisco SD-WAN Manager. The Embedded Wireless Controller on Cisco 1000 Series Integrated Services Routers helps you provide wireless connectivity without the need for another external controller to configure and manage the wireless settings on the routers using Cisco SD-WAN Manager.
Co-Management: Improved Granular Configuration Task Permissions	To provide a user with the ability to self-manage specific configuration tasks, you can assign the user permissions to configure specific features while excluding others. This feature introduces numerous new permission options, enabling fine granularity in determining which configuration task permissions to provide to a user.
RBAC for Security Operations and Network Operations Default User Groups	This feature provides the following default user groups: • network_operations user group for non-security policies • security_operations user group for security policies RBAC for policies allows you to create users and user groups with the required read and write permissions for security and non-security policies. Users can perform configuration and monitoring actions only for the authorized policy type.
Flexible Tenant Placement on Multitenant Cisco vSmart Controllers	With this feature, while onboarding a tenant to a multitenant deployment, you can choose the pair of multitenant Cisco SD-WAN Controller that serve the tenant. After onboarding a tenant, you can migrate the tenant to a different pair of multitenant Cisco SD-WAN Controller to allow for more tenant WAN edge devices than was forecast during onboarding.
Cisco Catalyst SD-WAN Routing	
Route Leaking between Inter-Service VPN	This feature allows you to leak routes between service VPNs on the same edge device. Route leaking feature allows redistribution of replicated routes between the inter-service VPN for Connected, Static, BGP, OSPF, and EIGRP protocols on Cisco IOS XE Catalyst SD-WAN devices.
Cisco Catalyst SD-WAN Policies	
Prioritized Color Preference	This feature adds support for ranking of Application Aware Routing (AAR) preferred and backup preferred colors. You can configure up to three levels of priority based on the color or path preference on a Cisco IOS XE Catalyst SD-WAN device.
Application-Aware Routing for IPv6	This feature enables you to configure application-aware routing (AAR) policies to operate with IPv6 application traffic.
Flexible NetFlow Export Spreading	This feature enables export spreading to prevent export storms that occur when a burst of packets are sent to external collector. The export of the previous interval is spread during the current interval to prevent export storms. When Deep Packet Inspection (DPI) or netflow packets are sent over a low-bandwidth circuit, the export spreading functionality is enabled to avoid packet drops.

Feature	Description
Support for Cisco SD-WAN Policy Configuration Tagging Using the Cisco vSmart Controller CLI Template	This feature allows you to group multiple policy objects under a tag. The tag mechanism when used in Cisco Catalyst SD-WAN centralized or localized policies: • Controls the policy configuration download speed between the Cisco SD-WAN Controller and the Cisco IOS XE Catalyst SD-WAN devices. • Improves management of the defined lists in the Cisco vSmart Controller. • Better organizes the configurations of the intent-based network.
Lawful Intercept	This feature enhances the support for Lawful Intercept in Cisco Catalyst SD-WAN. Cisco Catalyst SD-WAN's Lawful Intercept feature enables Cisco SD-WAN Manager and Cisco SD-WAN Controller to provide the key information to LEA so they can decrypt the Cisco Catalyst SD-WAN IPsec traffic captured by the MSP.
Cisco Catalyst SD-WAN Security	
Cisco SD-WAN Identity-Based Firewall Policy	This feature allows you to configure user-identity-based firewall policies for unified security policies. Cisco Identity Services Engine and Microsoft Active Directory Services are identity providers to authenticate and authorize device users in the network. When Cisco SD-WAN Manager and a Cisco SD-WAN Controller establish a connection to the Cisco Identity Services Engine, information about user and user groups—that is, identity-mapping information—is retrieved from the Cisco Identity Services Engine. Identity-based policies are then distributed to Cisco IOS XE Catalyst SD-WAN devices. This identity mapping information is used while creating firewall policies.
Automatic GRE Tunnels to Zscaler	With this feature, use the Secure Internet Gateway (SIG) feature template to provision automatic GRE tunnels to Zscaler SIGs. In earlier releases, the SIG template only supported the provisioning of automatic IPSec tunnels to Zscaler SIGs.
Global SIG Credentials Template	With this feature, create a single global Cisco SD-WAN Manager SIG Credentials template for each SIG provider (Cisco Umbrella or Zscaler). When you attach a Cisco SD-WAN ManagerSIG template to a device template, Cisco SD-WAN Manager automatically attaches the applicable global Cisco SIG Credentials template to the device template.
Monitor Automatic SIG Tunnel Status and Events	Monitor security events related to automatic SIG tunnels using the **Security Events** pane on the **Monitor** > **Security** page, and the **Events** dashboard on the **Monitor** > **Logs** page. Monitor automatic SIG tunnel status using the **SIG Tunnel Status** pane on the **Monitor** > **Security** page, and the **SIG Tunnels** dashboard on the **Monitor** > **Tunnels** page.
Disable Weak SSH Encryption Algorithms	This feature allows you to disable weaker SSH algorithms that may not comply with certain data security standards.
Cisco Catalyst SD-WAN Cloud OnRamp	

Feature	Description
Improved Visibility for Microsoft 365 Traffic	This feature provides improved visibility to allow you to monitor the details of Microsoft 365 traffic processed by Cloud OnRamp for SaaS.
Configure the Traffic Category and Service Area for Specific Policies	You can edit AAR policies individually to change the specified Microsoft 365 traffic category and service area for specific AAR policies.
Enable Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites	This feature allows you to selectively delete AAR policy sequences to exclude Cloud OnRamp for SaaS operation on specific applications at specific sites.
Option to Include or Exclude Microsoft Telemetry Data from Best Path Decision for Microsoft 365 Traffic	This feature allows you to choose whether Cloud OnRamp for SaaS should factor in the Microsoft telemetry data in the best path decision. If you disable this option, you can still view the Microsoft telemetry data in the Cisco SD-WAN Analytics dashboard, but it does not affect the best path decision.
Support for AWS GovCloud (US) with Cisco SD-WAN Cloud OnRamp for Multicloud	With the integration of Amazon Web Services (AWS) GovCloud (US) with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud, you can store your highly sensitive workloads in an isolated cloud that meets the Federal Risk and Authorization Management Program (FedRAMP) requirements of the U.S. government and its customers. The same features that are available with the AWS integration with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud are also available with Amazon GovCloud (US). Use the AWS Transit Gateway to connect your branch devices to the AWS GovCloud (US).
Support for the Azure for US Government Cloud with Cisco SD-WAN Cloud OnRamp for Multicloud	With the integration of the Azure for US Government cloud with Cisco Catalyst SD-WAN Cloud OnRamp for Multicloud, you can move and store your highly sensitive workloads in an isolated cloud that meets the Federal Risk and Authorization Management Program (FedRAMP) requirements of the U.S. government and its customers. All of the same features that are available for the Azure integration with Virtual WAN are also available with the Azure for US Government cloud.
Encrypted Multicloud Interconnects with Megaport	You can extend the SD-WAN fabric from the Interconnect gateway in Megaport into the AWS, Google Cloud and Microsoft Azure Cloud Service Providers.
Encrypted Multicloud Interconnects with Equinix	You can extend the SD-WAN fabric from the Interconnect gateway in Equinix into the AWS, Google Cloud and Microsoft Azure Cloud Service Providers.

Feature	Description
License Management for Cisco SD-WAN Cloud Interconnect with Megaport	To create Interconnect Gateways and Interconnect Connections in the Megaport fabric, you must purchase required licenses on Cisco Commerce Workspace. With this feature, Cisco SD-WAN Manager operates together with Megaport and enables you to monitor your licenses while Cisco and Megaport jointly enforce the license requirements when you create Interconnect Gateways or Interconnect Connections.
Decoupled Site-to-Site and Site-to-Cloud Connectivity Configuration for Cloud Gateways	With this feature, you can configure some cloud gateways to support site-to-site and site-to-cloud connectivity, and other cloud gateways to support only site-to-cloud connectivity. This configuration flexibility is particularly beneficial in some Google Cloud regions that do not yet support site-to-site connectivity. In earlier releases, connectivity type is a global configuration. You configure all the cloud gateways to support site-to-site and site-to-cloud connectivity, or to support only site-to-cloud connectivity.
Horizontal Scaling of Cisco Catalyst 8000V Instances in a Cloud Gateway	With this feature, you can deploy between two and eight Cisco Catalyst 8000V instances as part of a cloud gateway in a particular region. In earlier releases, you can deploy only two Cisco Catalyst 8000V instances as part of a cloud gateway, with each instance deployed in a different zone of a region.
Cisco Catalyst SD-WAN AppQoE	
HTTP Connect	Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, the HTTP Connect method handling is supported in AppQoE that enables services like SSL Proxy and DRE to optimize the HTTP Connect encrypted traffic.
Cisco SD-WAN Monitor and Maintain	
Access TAC Cases from Cisco SD-WAN Manager	This feature allows you to access Support Case Manager (SCM) wizard using Cisco SD-WAN Manager. You can create, view, or edit the support cases directly from Cisco SD-WAN Manager without having to go to a different Case Manager portal.
Analyze the Health of the Cisco SD-WAN Manager Cluster and Cluster Services Using the CLI	With this feature, you can analyze the health of the Cisco SD-WAN Manager cluster and the status of the cluster services using the **request nms cluster diagnostics** CLI command.
Additional Real Time Monitoring Support for AppQoE and Other Configuration Options	This feature adds support for real-time monitoring for AppQoE and other device configuration details. Real-time monitoring in Cisco SD-WAN Manager is similar to using **show** commands in the CLI of a device.
Customizable Monitor Overview Dashboard in Cisco SD-WAN Manager	This feature adds customizability to the **Monitor Overview** dashboard. It gives you the flexibility to specify which dashlets to view and sort them based on your personal preferences.

Feature	Description
Site Topology Visualization in Cisco SD-WAN Manager (Phase II)	This feature supports an enhanced, interactive visualization of site topology, providing information about the health of devices and tunnels in the topology. It provides you with an improved monitoring and troubleshooting experience.
Network-Wide Path Insight in Cisco SD-WAN Manager Enhancements	This feature provides enhancements to the network-wide path insight feature, including the collection and display of insight information, trace-level insight information, path insight information, and detailed application trace information.
IPv6 Support for Bidirectional Packet Capture on Cisco IOS XE SD-WAN Devices	This feature adds support for bidirectional capture of IPv6 traffic data to troubleshoot connectivity issues using CLI commands. As part of this feature, the following command is introduced to capture traffic details: monitor capture match ipv6
Compare Template Configuration Changes Using Audit Logs	This feature introduces a **Config Diff** option for audit logs of device templates and feature templates. The **Config Diff** option shows configuration changes made to the template, comparing the current configuration and previous configuration. The **Config Diff** option is available for audit logs to view the configuration changes when a template is not attached to a device.
Schedule the Software Upgrade Workflow	This feature introduces an option to schedule software upgrades for edge devices using Cisco SD-WAN Manager.
Software Upgrade Workflow Support for Additional Platforms	Added support for Cisco Enterprise NFV Infrastructure Software (NFVIS) and Cisco Catalyst Cellular Gateways.
Cisco Catalyst SD-WAN NAT	
Support for PPP Dialer Interfaces with NAT DIA	This feature adds support for the following Point-to-Point Protocol (PPP) dialer interfaces: PPP over Ethernet (PPPoE), PPP over Asynchronous Transfer Mode (PPPoA), and PPP over Ethernet Asynchronous Transfer Mode (PPPoEoA). You can use the PPP dialer interfaces to access IPv4 services and sites.
Support for Static NAT Mapping with HSRP	With this feature, if both the Hot Standby Router Protocol (HSRP) routers are configured with the same static NAT mapping, only the active device responds to the Address Resolution Protocol (ARP) request for a static NAT mapping entry. Traffic that fails over from the HSRP active device to the standby device does not have to wait for the ARP request to time out before failing over.
ALG Support for NAT DIA and Zone-Based Firewalls	This feature provides support for an application-level gateway (ALG) that translates the IP address inside the payload of an application packet. Specific protocols such as Domain Name System (DNS), FTP, and Session Initiation Protocol (SIP) require a NAT ALG for translation of the IP addresses and port numbers in the packet payload.

Feature	Description
Support for Port Forwarding with NAT DIA	With this feature, you can define one or more port-forwarding rules to send packets received on a particular port from an external network to reach devices on an internal network. Prior to Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and Cisco SD-WAN Manager, port forwarding was available for service-side NAT only.
Support for NAT High-Speed Logging	This feature provides the ability to enable or disable high-speed logging (HSL) of all translations by NAT. The new **ip nat log translations flow-export** command is introduced. You can configure NAT HSL using a device CLI or a CLI add-on template.
Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)	
Re-Origination Dampening	In networks experiencing instability, TLOCs and bidirectional forwarding detection (BFD) tunnels may cycle repeatedly between being available and unavailable. This causes the overlay management protocol (OMP) to repeatedly withdraw and re-originate routes. This churn adversely affects Cisco vSmart controller performance. Adding a delay before re-originating routes that have gone down repeatedly prevents excessive churn, and prevents this type of network instability from diminishing Cisco SD-WAN Controller performance.
Migrating to Multi-Region Fabric	Cisco Catalyst SD-WAN Multi-Region Fabric provides a migration mode to facilitate migrating an enterprise network to Cisco Catalyst SD-WAN. Migration mode enables a stepwise transition of devices from Cisco Catalyst SD-WANs that are not part of a Multi-Region Fabric network to Cisco Catalyst SD-WANs operating in a Multi-Region Fabric architecture. The migration mode is useful for migrating complex networks that function similarly to a Multi-Region Fabric architecture—that is, they have multiple network segments, and have a control policy that directs inter-segmental traffic through network hubs.
Match Traffic by Destination Region	When creating an application route policy or data policy, you can match traffic according to its destination region. The destination may be a device in the same primary region, the same secondary region, or neither of these.
Specify Path Type Preference	When configuring a centralized policy, you can create a preferred color group list, which specifies three levels of route preference, called primary, secondary and tertiary. The route preferences are based on TLOC color and, optionally, on the path type—direct tunnel, multi-hop path, or all paths. Path type is relevant to networks using Multi-Region Fabric.
High Availability	
Configure Disaster Recovery Alerts	This feature provides support for configuring Cisco SD-WAN Manager alerts to generate an alarm and a syslog message for any disaster recovery workflow failure or event that occurs.

New and Enhanced Hardware Features

New Features

- Support for Cisco IR8140 Heavy Duty Router: Cisco Catalyst SD-WAN capability can now be enabled on Cisco IR8140H and Cisco IR8140H-P Heavy Duty Routers.
- Support for Cisco DSL SFP Module: Cisco SD-WAN Manager CLI device templates now support the Cisco DSL SFP Module SFP-VADSL2+-I= for use with Cisco IR1101 Integrated Services Routers.
- Cisco Catalyst IR1800 Rugged Series Router support for Automotive Dead Reckoning (ADR): Cisco SD-WAN Manager now supports the configuration of ADR-GPS FRU for the Cisco Catalyst IR1800 Rugged Series Router platform using a CLI template. See GPS/Dead Reckoning module (IRM-GNSS-ADR).
- Cisco Catalyst IR1800 Rugged Series Router support for Ignition Power Management: Cisco SD-WAN Manager now supports the configuration of Ignition Power Management for the Cisco Catalyst IR1800 Rugged Series Router platform using a CLI template. See Ignition Power Management.
- Cisco Catalyst IR1835 Rugged Series Router support for General-Purpose Input or Output ports (GPIO): Cisco SD-WAN Manager now supports the configuration of GPIO for the Cisco Catalyst IR1835 Rugged Series Router platform using a CLI template. See Digital IO and Configuring Digital IO.

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.9.x

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.9.3a

Behavior Change	Description
Organizational Unit Field Not Required in Certificates for Edge Devices or Controllers	The signed digital certificates that you install on edge dev Catalyst SD-WAN overlay do not require the Organizatio However, if a signed certificate includes the Organizationa the organization name configured on the device. This is described in the Configure Enterprise Certificates

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.9.2a

Behavior Change	Description
A **show sdwan from-vsmart commit-history** command is added for verifying policy-related commit events and for analyzing the average time required for the policy commit.	A new command, show sdwan from-vsmart commit-histo
The **snmp-server subagent fetch count** command is used to fetch the entry count if an SNMP MIB table includes a large number of table entries.	A note is added in the Supported SNMP MIBs section.

Behavior Change	Description
The **Community Name** field has been removed from the SNMP feature. In its place, the **User Label** field has been added that helps you distinguish or update a community name when there are multiple community names for an SNMP target.	The new **User Label** field is described in the SNMP section. S the **Community Name** field.
An **Internet Outages** option is added to the **Analytics** menu in Cisco SD-WAN Manager.	The **Internet Outages** option is described in the Internet Out

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Behavior Change	Description
Support is added for adjusting the TCP maximum segment size (MSS) for a service VPN or for Network Address Translation (NAT) Direct Internet Access (DIA) use cases. Adjusting the TCP MSS value helps prevent TCP sessions from being dropped.	A note is added in the Configure TCP MSS and Clear Dont F A note is added in the Information About Using a Dialer Inter
A link is added from the Cisco SD-WAN Manager menu to the Cisco Catalyst SD-WAN Portal. From the Cisco Catalyst SD-WAN menu, click **SD-WAN Portal** to access the Cisco Catalyst SD-WAN Portal for provisioning, monitoring, and maintaining Cisco Catalyst SD-WAN controllers using public cloud providers.	A note is added in the Cisco Catalyst SD-WAN Solution sect
Support is added for configuration of a device access policy having only a default action and with no policy sequences. You can now create a device access policy with only a default action and with no policy sequences for creation of a device configuration or a Cisco SD-WAN Manager configuration for both protocols, Secure Shell (SSH) and Simple Network Management Protocol (SNMP).	A note is added in the Configure Device Access Policy Using
A list of valid characters is added. These characters must be used in the user ID, password, and the URL name or path when downloading an image from a remote server manually.	A note is added in the Upgrade the Software Image on a Dev
Support is added to configure unique local IPv6 addresses for Cisco SD-WAN Controller, Cisco SD-WAN Validator, and Cisco SD-WAN Manager controllers.	A note is added in the Configure the Cisco vSmart Controller
Support is added to calculate 8 bytes overhead based on the specified IP MTU value, to ensure that the configuration is pushed to the device.	A note is added in the Configure PPPoE using Cisco vManag
Support is added to manually enable or disable the unified logging fields in flexible netflow (FNF) using the **policy ip visibility features enable** command.	A note is added in the Unified Logging Security Connection Troubleshooting sections. A new command **policy ip visibility features enable** is adde

Behavior Change	Description
The **show sdwan omp routes** command now includes **tenant-id** and **verify** keywords.	The **show sdwan omp routes** command is updated.
We recommend that the Cisco SD-WAN Manager cluster interface should not be the same as the transport interface. Beginning with Cisco vManage Release 20.9.1, this is enforced. If you attempt to configure this, Cisco SD-WAN Manager displays an error message.	A note is added in the Guidelines for a Cisco vManage Cl
With the **Enable telemetry pull from and push to Microsoft** option enabled in Cisco SD-WAN Manager, the telemetry data that Cisco vAnalytics pulls from Microsoft to display in the Cisco vAnalytics dashboard now consists of the service area interface scores (1-100) and weight percentage for the score instead of the status (OK/NOT-OK/INIT).	A note is added in the Enable Application Feedback Metri
A new option **Traffic Steering** is available in Cisco SD-WAN Manager to aid Cisco IOS XE SD-WAN devices to determine the best path based on the telemetry data that Cisco vAnalytics pulls from Microsoft.	The new option **Traffic Steering** is updated in the Enable for Office 365 Traffic section.
A new option **Umbrella DNS Certificate** is available in Cisco SD-WAN Manager to upload and push to appropriate devices Umbrella root certificates for Umbrella DNS security.	The new **Umbrella DNS Certificate** option is described i Certificates section.
The IP address of an NTP server cannot be a broadcast or a multicast address.	A note is added in the Configure NTP section.
Cisco vManage Release 20.9.1 does not inadvertently change the transport mode of a device, which could interfere with the manual installation of HSEC licenses.	A note is added in the Restrictions for Managing License Policy section.
Use the **implicit-acl-on-bind-intf** command to enable implicit ACL protection on a physical interface in cases where a physical interface is not configured with a TLOC and bound to the loopback TLOC interface.	A note is added in the **Loopback TLOC Interface Boun** section in Information About Implicit ACL on Loopback
The Cisco SD-WAN Controller software version must be the same or be higher that the WAN edge device software version. If the WAN edge device software version is higher than the Controller software version, policy download to the device fails.	A note is added in Cisco SD-WAN Controller Compatibil Computing Resources.

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 this module.

- Cisco vManage Release 20.3.1 implements a hardened security posture to comply with FedRamp guidelines. As a result, your Cisco SD-WAN Analytics login credentials that are stored locally get erased on upgrading the software, and you cannot access the vAnalytics service directly through Cisco SD-WAN Manager. In this case, log in to Cisco SD-WAN Analytics using this URL: https://analytics.viptela.com. If you can't find your Cisco SD-WAN Analytics login credentials, open a case with Cisco TAC support.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, the **table** keyword is added to all show sdwan commands for which the output needs to be displayed in a tabular format. Using **| tab** is restricted for all Cisco Catalyst SD-WAN commands starting from Cisco IOS XE Catalyst SD-WAN Release 16.11.x.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, feature templates support the following network interface modules for Layer 3 features:
  - Cisco 2-port 100-Mbps/1-Gbps WAN Network Interface Module with 256-bit WAN MACsec (C-NIM-2T)
  - Cisco 1-port 2.5-Gbps/1-Gbps WAN Network Interface Module with Cisco UPoE (C-NIM-1M)
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, the Switch Port feature template supports an interface speed of 2500 Mbps when configuring a 2-Gigabit Ethernet interface for the following modules:
  - Cisco SM-X-16G4M2X and Cisco SM-X-40G8M2X EtherSwitch Service Modules on Cisco ISR 4000 Series Routers
  - Cisco C-SM-16P4M2X and Cisco C-SM-40P8M2X EtherSwitch Service Modules on Cisco Catalyst 8300 Series Edge Platforms
- **Cloud OnRamp for IaaS**: Beginning with Cisco vManage Release 20.9.1, we recommend setting up your cloud infrastructure using Cloud OnRamp for Multicloud. Cloud OnRamp for IaaS will be phased out in a future release.
- Beginning with Cisco vManage Release 20.9.1, you can add the route-target CLIs through the CLI add-on profile of a configuration group:

```
vrf definition Mgmt-intf
address-family ipv4
route-target export 119:512
route-target import 119:512
```

Resolved and Open Bugs

About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.5

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.5

Identifier	Headline
CSCwd42523	Same label is assigned to different VRFs.
CSCwe91898	Environmental syslog is not appearing when power cord is disconnected from the redundant PS
CSCwf51721	Enterprise Certificate status displayed as "Not Applicable" post rollback from viptela to ios-xe.
CSCwe31226	17.11: Issues/discrepancies around CPU alarms generated and sent to Cisco SD-WAN Manager from Cisco IOS XE Catalyst SD-WAN device.
CSCwe19034	Flooding of HSL packets
CSCwd01378	OMPD crash while withdrawing routes
CSCwf94294	Misprograming during vpn-list change under data policy.
CSCwh77221	The SNMP unable to poll SDWAN Tunnel Data after a minute.
CSCwf14727	FNF ucode crash when add or remove interface.
CSCwf39945	Device requested SLAC without customer issuing command.
CSCwf94052	BFD going down for newly onboarded Cisco IOS XE Catalyst SD-WAN device.
CSCwb79943	SDWAN-NAT Device ICMP replies should not be natted.
CSCwh53943	Dialer interface is blocking SIG Auto Tunnel workflow
CSCwc10244	While upgrading ISR4451 device generates fman fp core file.
CSCwf49597	Traffic is getting dropped with "SdwanDataPolicyDrop" with TunnelReason:MATCHED_NONE
CSCwe73993	Cisco IOS XE Catalyst SD-WAN device might reload during overlay session entry removal.
CSCwd66293	Traffic blackhole seen after few hours of soak due to Extra Key.
CSCwb74384	Cisco IOS XE Catalyst SD-WAN device: confd_cli high CPU utilization after executing "show sdwan app-route stats".
CSCwf21973	Device replying with NAT pool IP address instead of the WAN IP address.
CSCwh70449	PMTUD incorrectly converging without attempting to learn a higher MTU.
CSCwf95095	Intermittent BFD session flaps on Cisco IOS XE Catalyst SD-WAN device service side interface .

Identifier	Headline
CSCwf25249	The AppQoE DRE shows the optimized traffic is more than the original traffic on the data center SCs.
CSCwf65799	There is fpmd crash on device after Power ON when trying to sync the config.
CSCwh29805	The custom-app based policy triggering protocol deactivation and cpp traceback with traffic failure
CSCwi27324	Tunnels behind Sym-nat does not come up or flap after "clear omp all" trigger on HUB.
CSCwc83353	17.10: PPPoA dialer doesnt come up and randomly test case are failing when ran 174_aldi_script.
CSCwd20182	[SIT]:When firewall is enabled , speedtest with iperf server configured on vpn 0 fails.
CSCwe49684	Cisco Catalyst SD-WAN BFD sessions keeps flapping intermittently.
CSCwf71051	Issues seen due to race conditions between sdwan policy and og-mgr on config-change.

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.5

Identifier	Headline
CSCwd31983	[17.9-17.11] C1111-8P Inventory mismatch is seen after upgrading to 17.11.
CSCwh72441	The show sdwan appqoe aoim-statistics - APPQOE services restart
CSCwb74821	Cisco IOS XE Catalyst SD-WAN device: unexpected behavior due to unstable power source.
CSCwh94444	Post-upgrade checks didn't detected weak crypto config command esp-null leading to network outage.
CSCwi31523	EPBR FIA is not enabled on Port-channel sub-interface.
CSCwh63864	Service-side NAT Translation discrepancy
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites.
CSCwf40849	Cisco IOS XE Catalyst SD-WAN device IPv6: removing "advertise aggregate" configuration does not remove the entry from OMP.
CSCwd97769	Encryption supported still shows AES_256_CBC in security info of Cisco IOS XE Catalyst SD-WAN device.
CSCwa19332	Fragmeneted packets getting dropped unexpectedly when second fragment packet no translate.
CSCwf44703	Cisco IOS XE Catalyst SD-WAN device: NAT64 prefix is not originated into OMP
CSCwi07137	Crash when traffic is sent to UTD
CSCwi58561	Cisco IOS XE Catalyst SD-WAN Device : Tracker not working after software upgrade

Identifier	Headline
CSCwf73123	BFD timers reverting back to default value after negotiating correctly
CSCwh39906	Cisco IOS XE Catalyst SD-WAN device: confd_cli may cause high cpu. Parent PID of "confd_cli" containing "show ip fib"
CSCwi59854	'show sdwan policy service-path' command gives inconsistent results with app name specified.
CSCwh65016	Unexpected Reboots on Cisco IOS XE Catalyst SD-WAN device due to QFP exception
CSCwi51381	TrapOID of ciscoSdwanBfdStateChange is different from MIB file.
CSCwi32044	Device reboot due to "Critical process vip_confd_startup_sh"
CSCwi15688	Unexpected NAT translation occurs in a specific network.
CSCwe25926	Tracker group is down if one of the tracker elements is not reachable.
CSCwi60266	Cisco IOS XE Catalyst SD-WAN device with enterprise certificates not forming control connections with controllers after upgrade
CSCwi62230	SIG tunnel: 'SIG STATEâ is showing blank value.
CSCwe64991	Cisco SD-WAN Manager is reporting abnormal latency & jitter parameters
CSCwi19875	Cisco IOS XE Catalyst SD-WAN device is unable to process hidden characters in a file while trying to use bootstrap method

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.4a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.4a

Bug ID	Description
CSCwh87343	Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.4

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.4

Identifier	Headline
CSCwd45508	Cisco IOS XE Catalyst SD-WAN device does not form BFD across Serial link when upgrading from 17.3.3 to 17.6.x
CSCwd41236	On C8200-1N-4T, sh version points to /harddisk/core dir, but file is present in /bootflash/core dir
CSCwe93905	NAT ALG is changing the Call-ID within SIP message header causing calls to fail

Identifier	Headline
CSCwe28204	Catlayst 8500L: Control connection over L3 Tloc extension failing as no NAT table entry created
CSCwe43341	TLS control-connections down, traffic from controller dropped with SdwanImplicitAclDrop
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 device
CSCwe69572	Zscaler SIG: Tunnels don't come up with Custom Data Center IP
CSCwd87195	NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support.
CSCwe58264	TLOC down post ios-xe to viptela Nutella migration when enterprise cert used
CSCwd34941	NAT configuration with no-alias option is not preserved after reload
CSCwe81991	fugazi crash with qfp-ucode-fugazi in C8500L at @posix_mempool_prime_cache
CSCwe23276	Change in the IPsec integrity parameters breaks the connectivity
CSCwd49309	17.10: ucode crash seen on Thorium with traffic pointing to segfault in coff handler
CSCwe31471	Segmentation fault in SDWAN PB rx when per-tunnel qos config withdraw
CSCwe49009	Cisco IOS XE Catalyst SD-WAN device Router Crashes in "ftmd" Process When Configuring Tunnel "mode" or "route-via"
CSCwe70374	c8300/85000 platform punt-policer is not configurable
CSCwe18058	Unexpected reload with IPS configured on 17.6.3a
CSCwe73653	Cisco IOS XE Catalyst SD-WAN device router crashing due to memory leak in ftmd
CSCwd66293	Traffic blackhole seen after few hrs of soak due to Extra Key
CSCwe85421	Cisco IOS XE Catalyst SD-WAN device BFD Session Down with interface flap
CSCwd81262	Restrict option does not work when traffic match both Data policy and AAR policy
CSCwe15537	Cisco IOS XE Catalyst SD-WAN device:After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.
CSCvy23366	C8300-2N2S + UCSE: Kernel crash on C8300-2N2S with UCSE module.
CSCwe70642	AAR overlay actions are applied to DIA traffic
CSCwe79007	Cisco IOS XE Catalyst SD-WAN device unexpected reload when doing ips test with UTD ips engine
CSCwe09341	TLOC down post viptela to ios-xe Nutella migration when enterprise cert used

Identifier	Headline
CSCwf16608	Cisco IOS XE Catalyst SD-WAN device configured with 10G BDI might reload when running NWPI Trace with QoS Insight enabled
CSCwf26771	Invalid L4 Header drop due to multiple encap
CSCwd79572	FW policy with app-family rule with FQDN causes traffic drop for other sequences
CSCwf37888	Cisco IOS XE Catalyst SD-WAN device Packet Duplication: Duplicate packets are counted on Primary Tunnel Interface Statistics.

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.4

Identifier	Headline
CSCwf51144	Zombie confd_cli processes hanging around are maxing out CPU
CSCwc86434	Static NAT DIA inside static routes being advertised over OMP to remote sites
CSCwf40849	Cisco IOS XE Catalyst SD-WAN device IPv6: removing "advertise aggregate" configuration does not remove the entry from OMP
CSCwd01378	OMPD crash while withdrawing routes
CSCwc83353	17.10: PPPoA dialer doesnt come up and randomly test case are failing when ran 174_aldi_script
CSCwd53710	17.10 - Crash seen when umbrella/zscaler template pushed to device when name_lookup takes > 30 sec
CSCwf45486	OMP to BGP Redistribution Leads to Incorrect AS_Path Installation on Chosen Next-Hop
CSCwf21973	Device replying with NAT pool IP address instead of the WAN IP address
CSCwd97769	Encryption supported still shows AES_256_CBC in security info of Cisco IOS XE Catalyst SD-WAN device
CSCwf44703	Cisco IOS XE Catalyst SD-WAN device: NAT64 prefix is not originated into OMP
CSCwd20182	[SIT]:When firewall is enabled , speedtest with iperf server configured on vpn 0 fails.
CSCwf39945	Device requested SLAC without customer issuing command
CSCwf35823	c1121-4P / 17.6.2 / "ip nat settings central-policy" dropping service side NAT traffic after reboot

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.3a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.3a

Identifier	Headline
CSCwc68069	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature
CSCwc76082	check_sig_ipsec_ike_sessions fails with could not find entry for Tunnel100001
CSCwe00946	Cisco Catalyst SD-WAN | System crash after disabling endpoint-tracker on tunnel interfaces
CSCwc48427	[SITLite] BFD issues with clear_omp -> non-PWK + non-VRRP scenario only
CSCwd15560	With 2 sequences, should not skip if the match is different and action is same
CSCwd71656	17.10 Auto GRE- After reboot, no ip address assigned to destination address for 1 tunnel
CSCwd12955	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured
CSCwd67198	17.10: uCode crash seen on Curie 2RU after stopping NWPI trace
CSCwd47940	Cisco IOS XE Catalyst SD-WAN device: PMTU Discovery is not working after interface flap
CSCwb32635	17.6.2 IOS XE SD-WAN - tech files are incomplete when running admin-tech
CSCwe29430	[SIT] ISR4221X/K9 : Critical process fpmd fault on rp_0_0 (rc=134)
CSCwd34573	Sparrow crashed: fman_fp_image: QFP0.0 CPP Driver LOCKDOWN encountered due to previous fatal error
CSCwd15070	Cisco IOS XE Catalyst SD-WAN device upgrade fails and can't change template due to "advertise aggregate" config w/o prefix-list
CSCwc77003	Prefix through hub not intalled in FIB, with OD Tunnels, seeing drops due to FirewallPolicy
CSCwe06507	Cisco IOS XE Catalyst SD-WAN device drops packets with reason 55 (Forus) when port forwarding is enabled from outside to inside
CSCwd44006	Control Connection on Cisco IOS XE Catalyst SD-WAN device doesn't come-up with reverse proxy using Enterprise Certificate
CSCwd71586	BFD sessions flapping on an interface with SYMNAT may lead to IPSec crash
CSCwd44439	ASR and c8500 crashing at fman_sdwan_nh_indirect_delete_from_hash_table
CSCwd14061	FTM is shooting up high and stuck in loop with the function ftm_sa_add().

Identifier	Headline
CSCwd44586	Cisco IOS XE Catalyst SD-WAN device - Login banner config is changed after upgrade to 17.6.3a
CSCwd01326	Catalyst 8500L - qfp-ucode-fugazi crashes with SIGABRT within cio infra under heavy load

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.3a

Identifier	Headline
CSCwd42523	Same label is assigned to different VRFs
CSCwd45508	Cisco IOS XE Catalyst SD-WAN device does not form BFD across Serial link when upgrading from 17.3.3 to 17.6.x
CSCwd76364	Cisco IOS XE Catalyst SD-WAN device crash with imgr_n2_ipsec_sa_ctx_register
CSCwe23276	Change in the IPsec integrity parameters breaks the connectivity
CSCwd97350	Cisco IOS XE Catalyst SD-WAN device did not created a crash file after Critical software exception
CSCwe18058	Unexpected reload with IPS configured on 17.6.3a
CSCwe28204	Cisco Catalyst 8500L: Control connection over L3 Tloc extension failing as no NAT table entry created
CSCwd90056	C8500-12X4QC P2MP WAN MACSEC does not allow traffic to pass on the link
CSCwe19394	Cisco IOS XE Catalyst SD-WAN device: device may boot up into prev_packages.conf due to power outage
CSCwe27241	nbar classification error with custom app-aware routing policy
CSCwd53710	17.10 - Crash seen when umbrella/zscaler template pushed to device when name_lookup takes > 30 sec
CSCwe32140	Nutella Cisco IOS XE Catalyst SD-WAN device do not accept the password via netconf
CSCwe09341	TLOC down post viptela to ios-xe Nutella migration when enterprise cert used
CSCwd79572	FW policy with app-family rule with FQDN causes traffic drop for other sequences
CSCwd10988	Cisco IOS XE Catalyst SD-WAN device crashes due to OMP process
CSCvy53031	Inconsistent behavior found when adding tunnel source config to virtual-template interface
CSCwe24654	Cisco IOS XE Catalyst SD-WAN device app-route Stats Show 100 percent loss but tunnel was up
CSCwd34941	NAT configuration with no-alias option is not preserved after reload

Identifier	Headline
CSCwd97774	CFLOWD egress INFT shows NULL when tunnel is sourced with loopback

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.2a

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.2a

Identifier	Headline
CSCwb65396	C1116-4P: CLI template push fails with error: 'Error: on line 48: line-mode single-wire line 0'
CSCwc23077	Firewall drop seen stating “FirewallL4” seen on Cisco IOS XE Catalyst SD-WAN Device
CSCwb32059	Cellular interface tracker down but NAT route persists in the Service VPN Routing Table
CSCwc44851	Bootstrap failing on c8300 on 17.9
CSCwc96444	Cisco IOS XE Catalyst SD-WAN Device router is not programming correct next-hop for unicast prefix with multicast config present
CSCwc89328	Multiple C8500s on Cisco SD-WAN experienced crashes every 4-5min
CSCwd06118	IKEv2 Cert-based IPSEC not working between Cisco IOS-XE and AWS
CSCwc77183	Packet duplication is causing drops in payment transactions with Cisco SD-WAN GenericDrop code.
CSCwc20170	C8500 cEdgeCisco IOS XE Catalyst SD-WAN Device Reloads Unexpectedly due to Critical FTMD Fault when VRF Configuration is Pushed
CSCwd45894	Cisco Catalyst SD-WAN ACL TCAM not in sync with configuration
CSCwc52538	Cisco SD-WAN flows are not distributed and load-balanced evenly and consistently
CSCwc45950	ZBFW self zone policy drops ssh session on Mgmt-intf 512 ports
CSCwb90252	Automatically freeing up filesystems stale image or recovered folder (lost+found)
CSCwc79145	Throughput degrades when local TLOC specified in Data Policy goes down
CSCwc32595	BFD sessions remains down if interface flap form up/down/up
CSCwb48953	Cisco IOS XE Catalyst SD-WAN Device speed test failing with "Device Error: Speed test in progress"
CSCwd11365	Needs cert update - Azure CGW creation fails due to NVA provisioning failure
CSCwc95218	C8300 with 5G module P-5GS6-GL is losing cellular config at each boot after upgrading to 17.9.1

Identifier	Headline
CSCwc28587	C8300 : Crashed without generating any core (Critical process plogd fault on rp_0_0 (rc=75)
CSCwd13352	SSH from Cisco SD-WAN Manager vshell to Cisco IOS XE Catalyst SD-WAN Device getting closed after Cisco IOS XE Catalyst SD-WAN Device update.
CSCwc77177	BFD and control packets are dropped when ACL is applied on gigi to which loopback is bind
CSCwc68132	SIG tunnel tracker packets are dropped by firewall with self zone policy
CSCwb67406	The IPSLA udp-jitter V3 (optimize timestamp+precision microseconds) does not work on C8500

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.2a

Identifier	Headline
CSCwd45508	Cisco IOS XE Catalyst SD-WAN Device does not form BFD across Serial link when upgrading from 17.3.3 to 17.6.x
CSCwd33966	Unable to configure the local BGP as-path-list via Cisco SD-WAN Manager.
CSCwa14636	Cisco IOS XE Catalyst SD-WAN Device stopped forwarding traffic. Suspect OMPD is busy
CSCwd15560	With 2 sequences, should not skip if the match is different and action is same
CSCwd13050	After upgrade to Cisco Cisco SD-WAN Manager Release 20.6.3, Cisco IOS XE Catalyst SD-WAN Device moved into Out of Sync status on Cisco SD-WAN Manager.
CSCwd12955	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured
CSCwd37410	0365 and MS Teams applications access issues when using DIA with app-list match in data-policy
CSCwd36621	Cisco IOS XE Catalyst SD-WAN Device: CERM may kick in due to IPSec sessions initiated for on-demand tunnels
CSCwd44586	Cisco SDWAN Cisco IOS XE Catalyst SD-WAN Device - Login banner config is changed after upgrade to 17.6.3a
CSCwd44006	Control Connection on Cisco IOS XE Catalyst SD-WAN Device doesn't come-up with reverse proxy using Enterprise Certificate
CSCwd29334	Upgrade failures due to inability to establish netconf connection from Cisco SD-WAN Manager to upgrade-confirm
CSCwd34941	NAT configuration with no-alias option is not preserved after reload

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

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

Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Identifier	Headline
CSCwb43423	Cisco IOS XE Catalyst SD-WAN Device image installation fails
CSCwb16723	Traceroute not working on Cisco IOS XE Catalyst SD-WAN Device with NAT
CSCwa67886	UDP based DNS resolution doesn't work with IS-IS EMCP on Cisco IOS XE Catalyst SD-WAN Device
CSCwb33968	Cisco Cisco SD-WAN Manager failed to display active flows when flow count is high on the device.
CSCvz84588	Destination prefix packets getting dropped because forwarding plane is not programming the next hop.
CSCwb59736	CSR BFD tunnel are zero with Cisco Catalyst SD-WAN version 17.03.03.0.7
CSCwb44275	Simulated flows with PPPoE with NAT DIA result in crash consistently
CSCwa57873	Incorrect reload reason - Last reload reason: LocalSoft for Netconf Initiated request
CSCwb51595	Missing IOS config (voice translation rule) on upgrade from 17.3 to 17.6
CSCwb18315	Umbrella DNS security policy doesn't work with Cloud onRamp with SIG tunnels
CSCwa49721	Cisco Catalyst SD-WAN HUB with firewall configured incorrectly dropping return packets when routing between VRFs
CSCwb18223	SNMP v2 community name encryption problem
CSCwb39098	Router crashed after new IPv6 address assigned when router use specific configuration

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Identifier	Headline
CSCwc32595	bfd sessions remains down if interface flap form up/down/up
CSCwc20075	Unable to switch the technology from 4g to 3g
CSCwc38529	[17.6] Traffic seems not inspected by UTD when umbrella is set
CSCwc55467	BFD Tunnel on Cisco SDWAN router is not staying up, 1 out of 40 tunnels.
CSCwc20170	C8500 Cisco IOS XE Catalyst SD-WAN Device reloads unexpectedly due to critical FTMd fault when VRF configuration is pushed

Identifier	Headline
CSCwc37465	Static NAT configuration in CLI with the no-alias keyword cannot be retrieved via NETCONF/YANG
CSCwc27208	BFD sessions not coming UP because of ANTI-REPLAY-FAILURES
CSCwc06047	Cisco Catalyst SD-WAN tunnel keeps on flapping on dialer interface with 17.3.6 throttle image for TSN platform
CSCwc63337	Destination not reachable if configured as a next for a static route resolvable via non /32 OMP
CSCwc52538	Cisco Catalyst SD-WAN flows are not distributed and load-balanced evenly and consistently
CSCwc23077	Firewall drop seen stating “FirewallL4” seen on Cisco IOS XE Catalyst SD-WAN Device
CSCwb74821	Yang-management process confd is not running, controller mode 17.6.2a
CSCwb67406	The IPSLA udp-jitter V3 (optimize timestamp+precision microseconds) does not work on C8500
CSCwc53885	Cisco IOS XE Catalyst SD-WAN Device "no ip nat" config is allowed to be committed and removes nat routes among other nat config
CSCwc59650	show sdwan app-fwd cflowd flows vpn X format tabled does not show all flows for vpn X
CSCwc44851	Bootstrap failing on c8300 on 17.9
CSCwc55684	Cisco Catalyst SD-WAN SIG GRE: Layer 7 Health check doesn't work on Loopback interfaces
CSCwc42978	ISR1100-4G looses all BFD sessions with Invalid SPI
CSCwc54463	Cisco IOS XE Catalyst SD-WAN Device C1121x-8P LAN Module is down when high CPU noticed
CSCwc55260	Cisco Catalyst SD-WAN - Memory leak due to FTMd process

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 changes between Cisco vManage 20.8.x and Cisco vManage Release 20.9.1.

Workflows Menu

In Cisco vManage Release 20.9.1, the following changes have been made to the **Workflows** menu:

- The **Launch Workflows** submenu is renamed as **Workflow Library**.
- The **Popular Workflows** section is introduced for easy and quick access to the workflows.

Figure 1: Workflows Menu in Cisco SD-WAN Manager 20.8.x

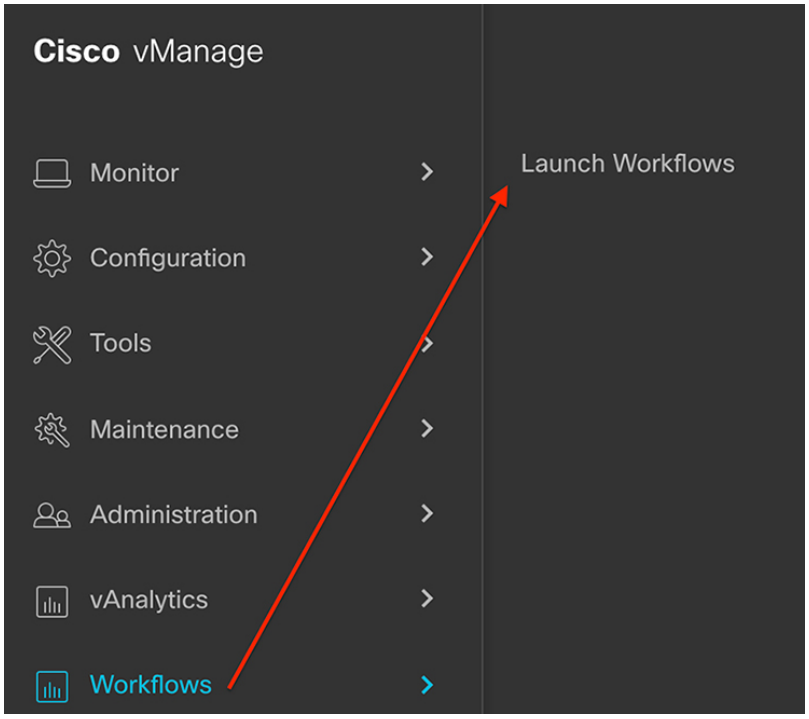
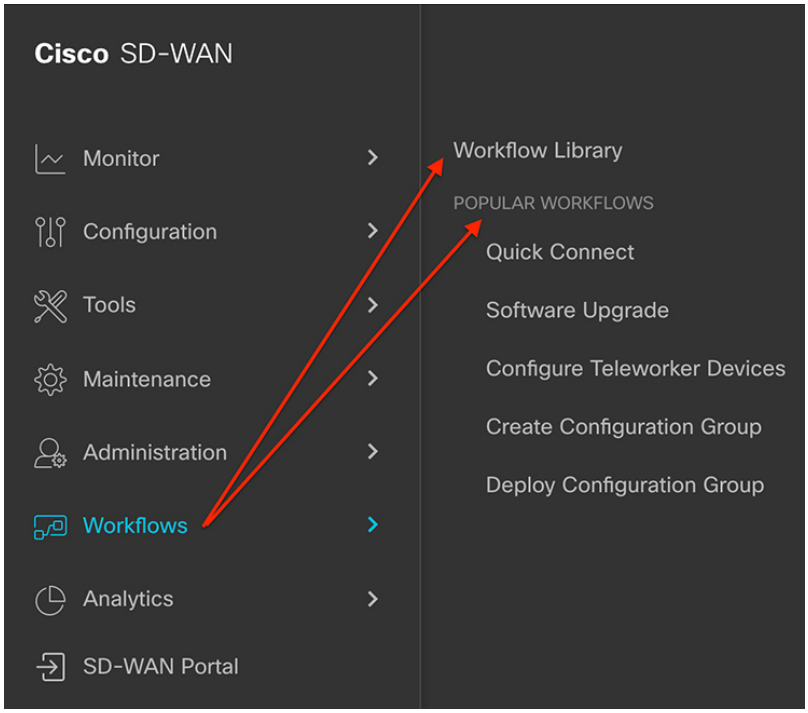


Figure 2: Workflows Menu in Cisco SD-WAN Manager 20.9.1



- The **Rapid Site Configuration Group** and **Custom Configuration Group** workflows are removed, and the **Create Configuration Group** workflow is introduced.

Figure 3: Rapid Site Configuration Group Workflow in Cisco SD-WAN Manager 20.8.x

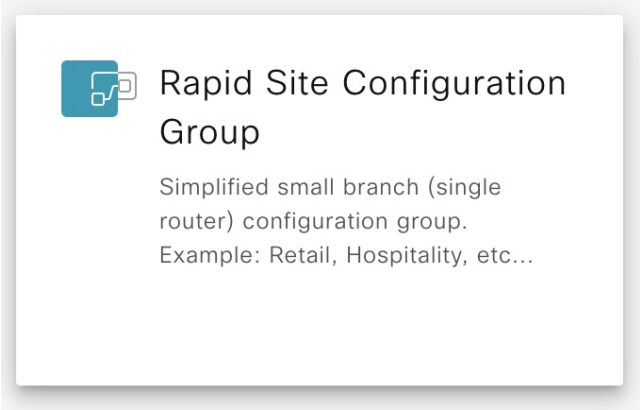


Figure 4: Custom Configuration Group Workflow in Cisco SD-WAN Manager 20.8.x

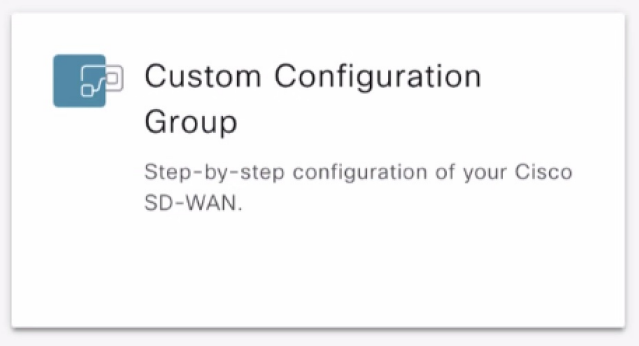
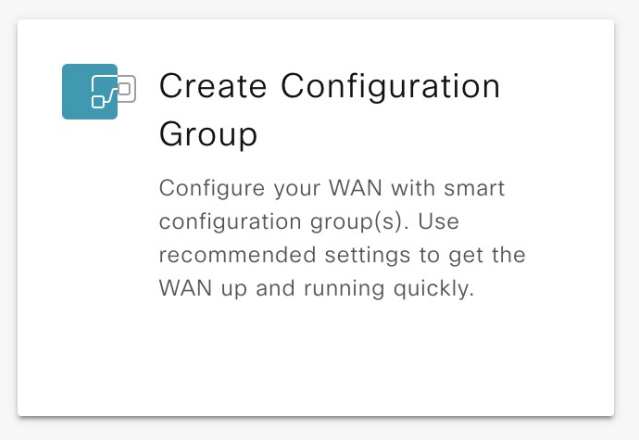


Figure 5: Create Configuration Group Workflow in Cisco SD-WAN Manager 20.9.1



- The **Provision WAN Sites and Devices** workflow is renamed as **Deploy Configuration Group**.

Figure 6: Provision WAN Sites and Devices Workflow in Cisco SD-WAN Manager 20.8.x

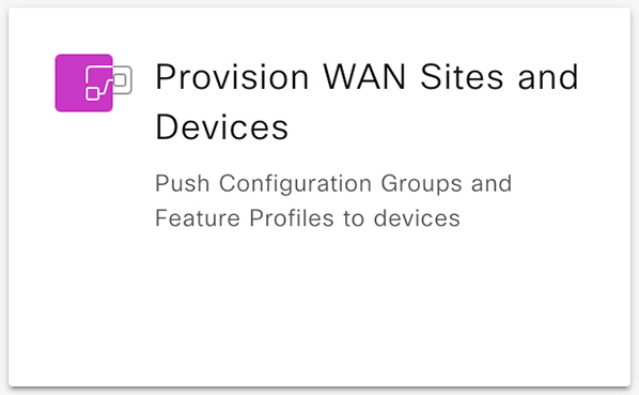
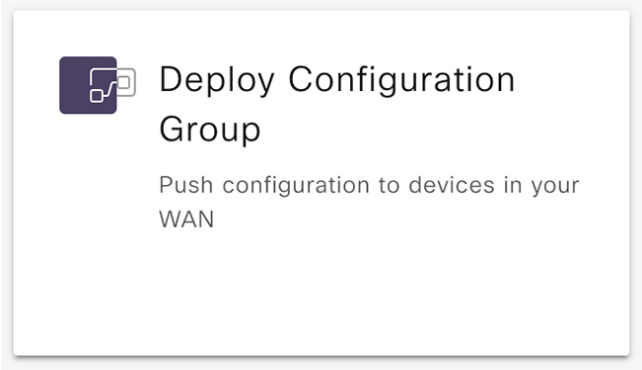


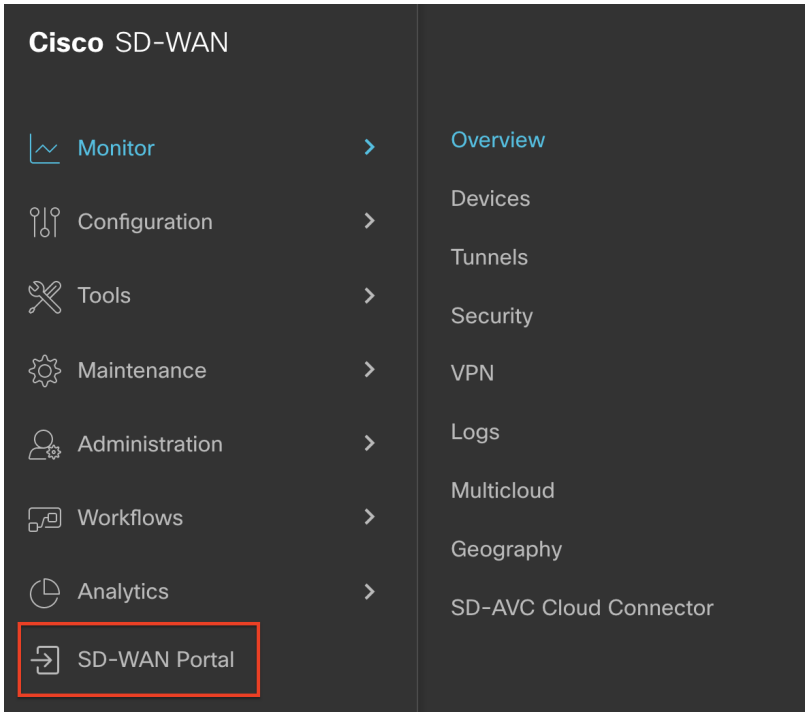
Figure 7: Deploy Configuration Group Workflow in Cisco SD-WAN Manager 20.9.1



SD-WAN Portal Menu

In Cisco vManage Release 20.9.1, **SD-WAN Portal** is added to the Cisco SD-WAN Manager menu. Choose **SD-WAN Portal** to access the Cisco SD-WAN Self-Service Portal.

Figure 8: SD-WAN Portal Menu in Cisco SD-WAN Manager 20.9.1



Monitor Overview Page

In Cisco vManage Release 20.9.1, the labels of the following UI elements have changed:

- **Devices** to **WAN Edges**
- **Device Health** to **WAN Edge Health**

- **Device Inventory** to **WAN Edge Inventory**

Figure 9: Monitor Overview Page in Cisco SD-WAN Manager 20.8.x

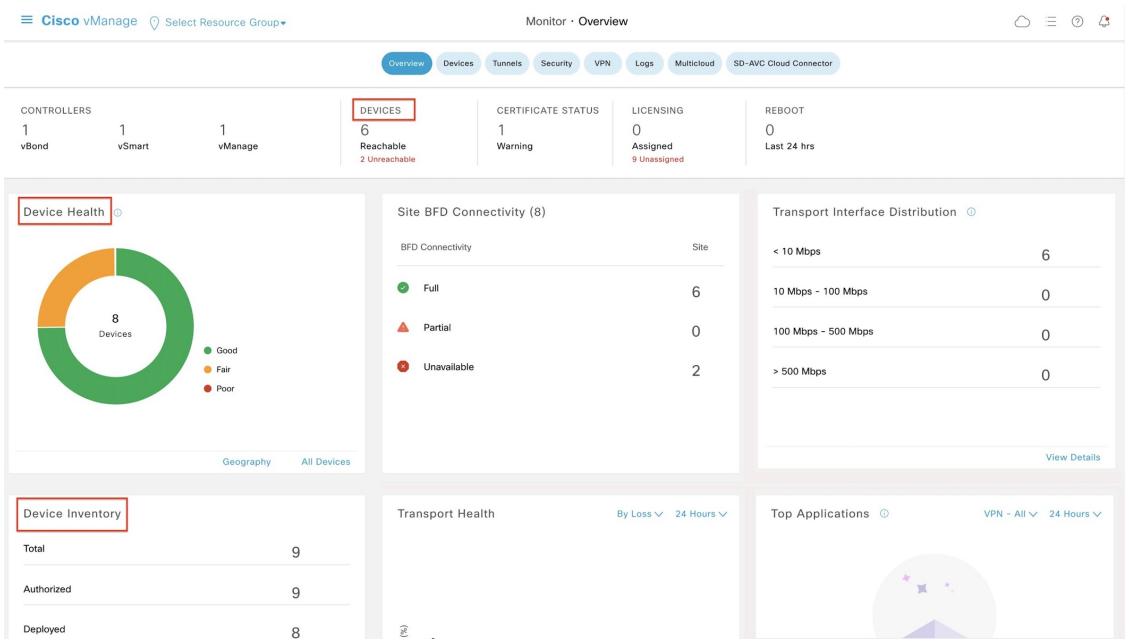
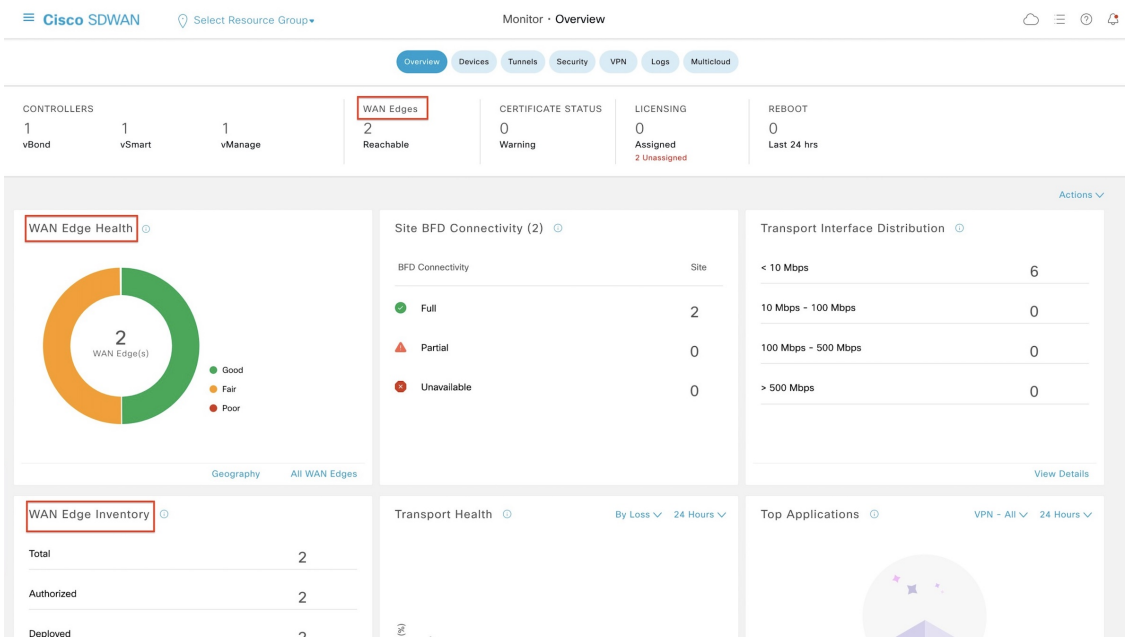


Figure 10: Monitor Overview Page in Cisco SD-WAN Manager 20.9.1



Monitor VPN Page

In Cisco vManage Release 20.9.1, the labels of the following UI elements have changed:

- **Device Status** to **WAN Edge Reachability**

- **Device Health** to **WAN Edge Health**

Figure 11: Monitor VPN Page inCisco SD-WAN Manager 20.8.x

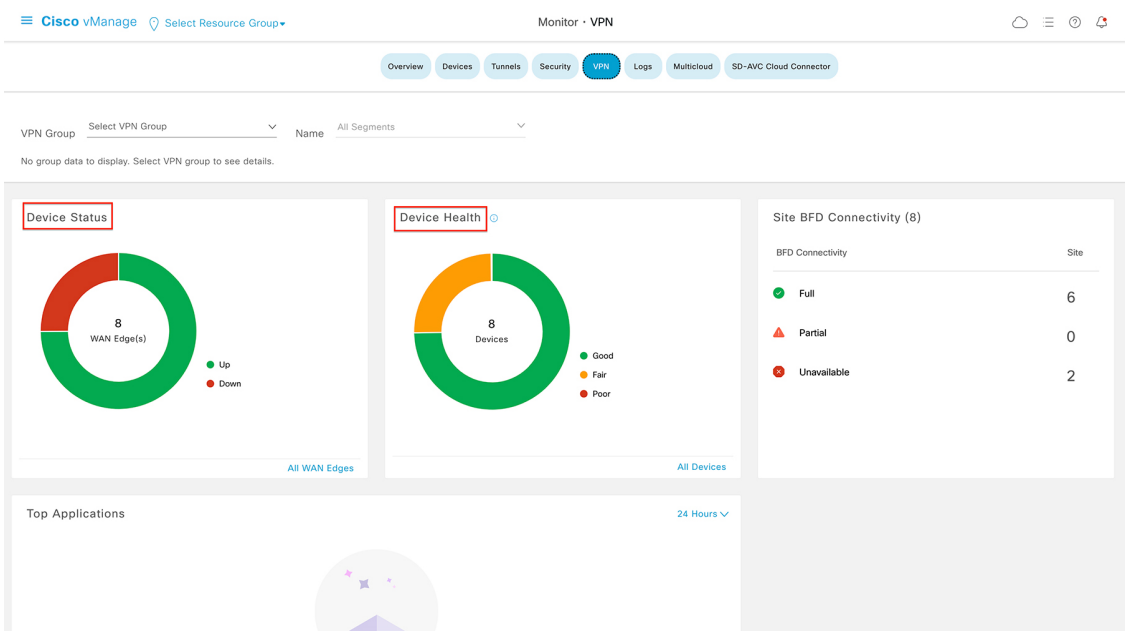
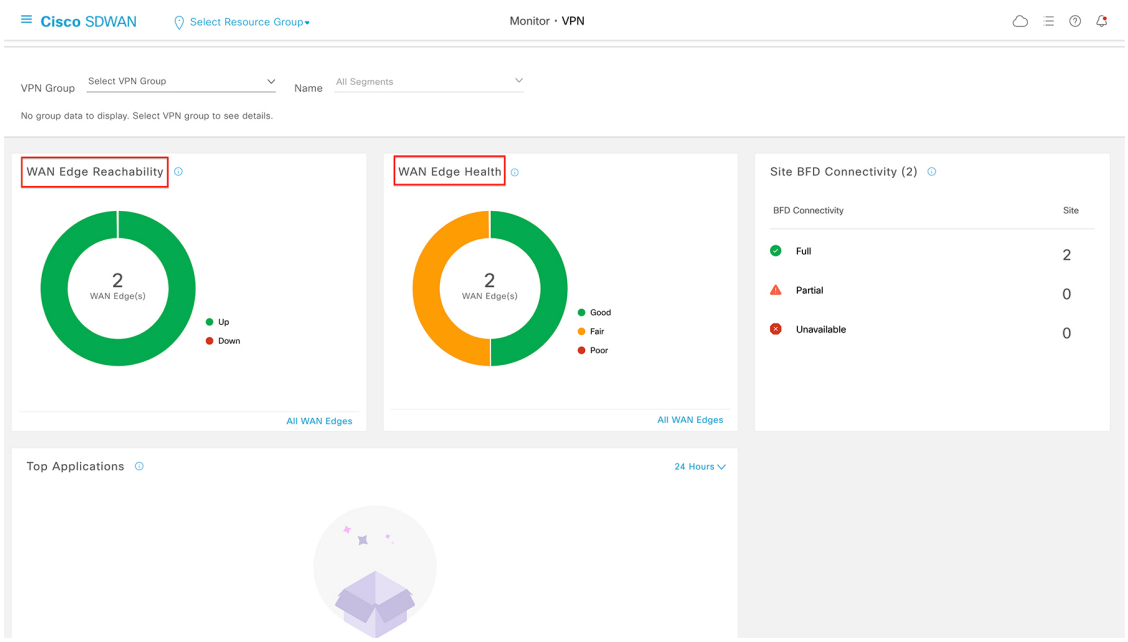


Figure 12: Monitor VPN Page in Cisco SD-WAN Manager 20.9.1



Configuration Groups Edit Page

In Cisco vManage Release 20.9.1, the feature profiles are presented in a tabular format, thereby enabling you to scan all the profiles at once. In Cisco vManage Release 20.8.x, the feature profiles were organized in a card-based presentation.

Figure 13: Configuration Groups Edit Page in Cisco SD-WAN Manager 20.8.x

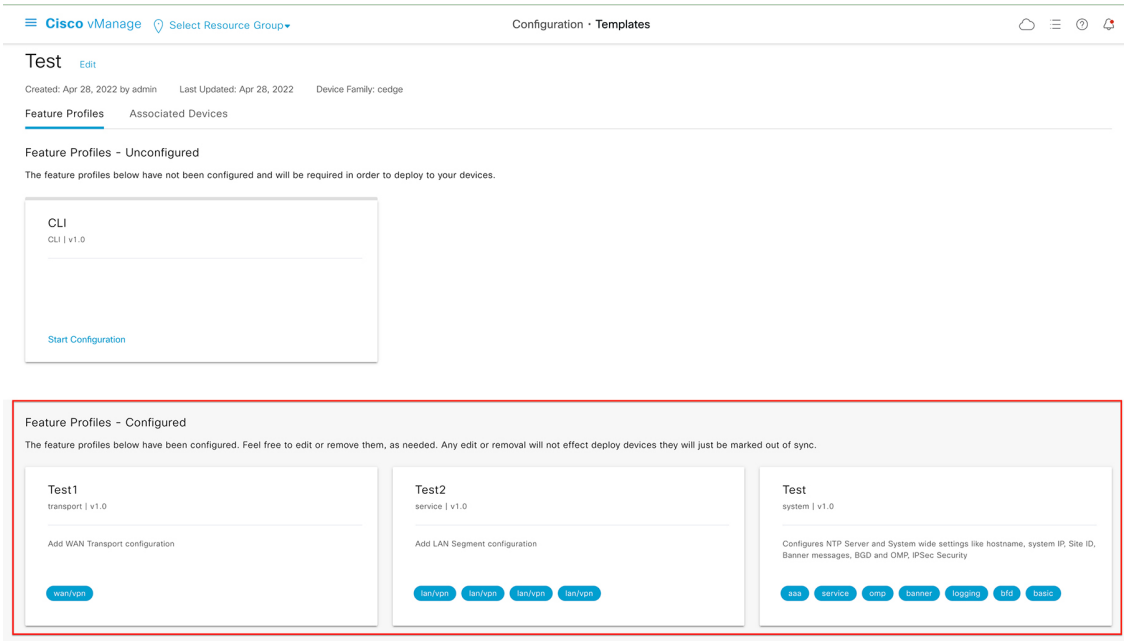
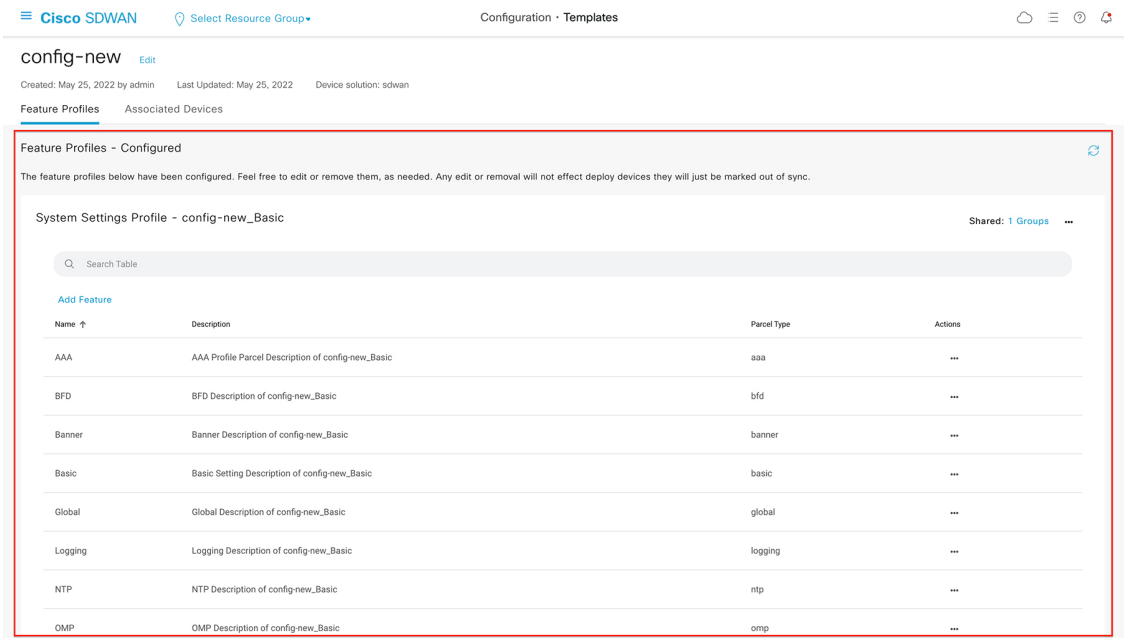


Figure 14: Configuration Groups Edit Page in Cisco SD-WAN Manager 20.9.1



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