

# 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:** 2025-04-30

## 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.

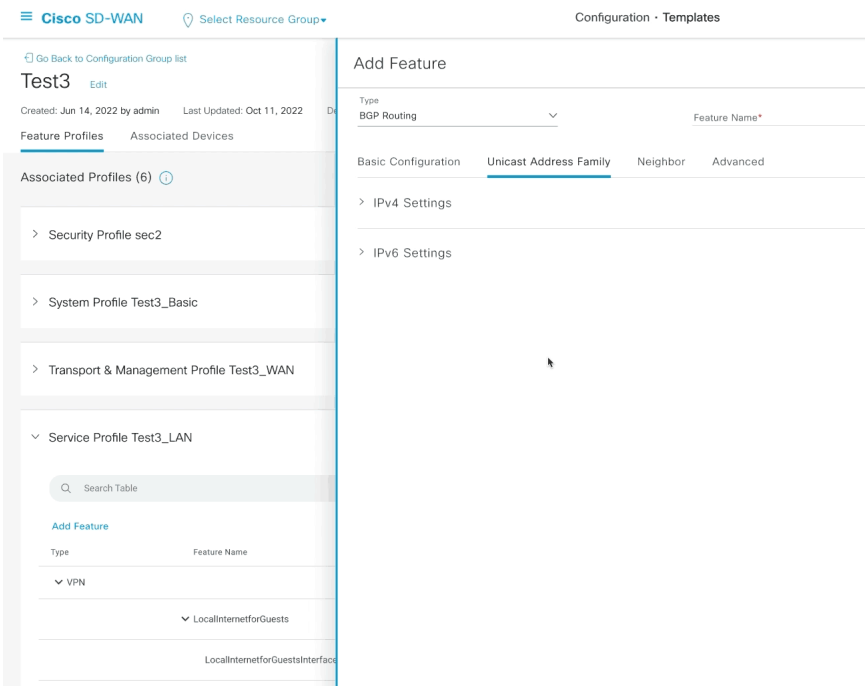
**Table 1: Cisco IOS XE Catalyst SD-WAN Release 17.9.4**

Feature	Description
<b>Cisco Catalyst SD-WAN Analytics</b>	
<a href="#">Easy Onboarding of Cisco SD-WAN Analytics into Cisco Catalyst SD-WAN Manager</a>	This feature enables you to easily onboard Cisco SD-WAN Analytics into Cisco Catalyst SD-WAN Manager.

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

Feature	Description
<b>Cisco Catalyst SD-WAN Systems and Interfaces</b>	

Feature	Description
Changes in the <b>Add Feature</b> and <b>Edit Feature</b> Forms	

Feature	Description
	<p>The following enhancements are introduced in the <b>Add Feature</b> and <b>Edit Feature</b> forms.</p> <ul style="list-style-type: none"> <li>• Accordion menus have been introduced to reduce scrolling. Click an accordion or the corresponding header to show or hide the content associated with it.</li> </ul>  <ul style="list-style-type: none"> <li>• A common template has been introduced to present repeated data.</li> </ul>

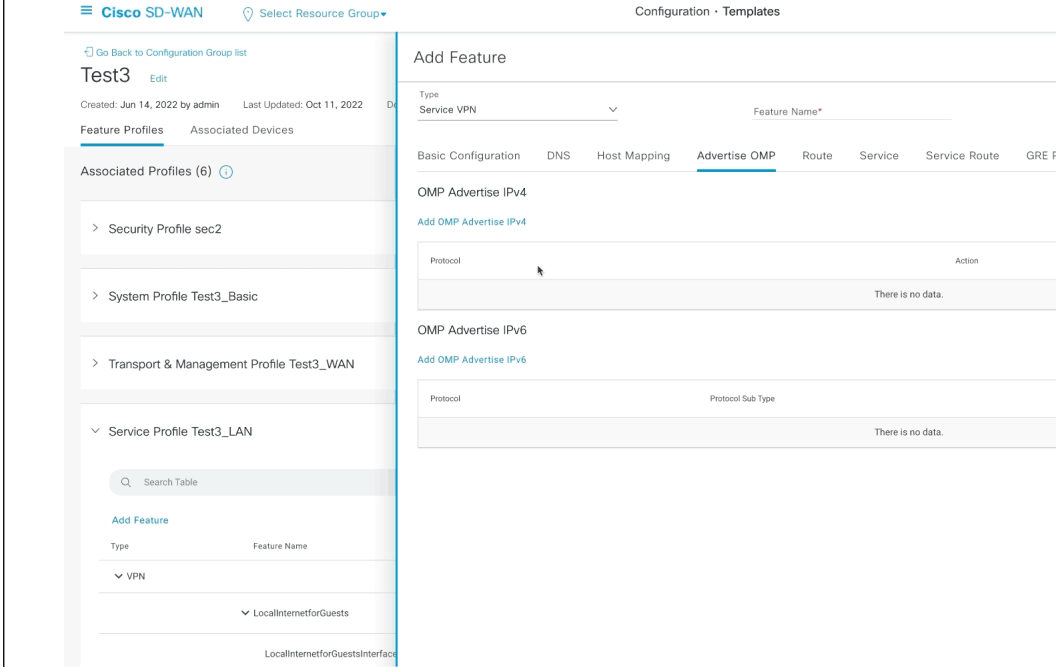
Feature	Description
	 <p>The screenshot displays the Cisco SD-WAN configuration interface. On the left, the 'Test3' configuration group is shown with its associated profiles: Security Profile sec2, System Profile Test3_Basic, Transport &amp; Management Profile Test3_WAN, and Service Profile Test3_LAN. The 'Add Feature' dialog is open, showing the 'Service VPN' type and the 'Advertise OMP' tab. The dialog includes sections for 'OMP Advertise IPv4' and 'OMP Advertise IPv6', each with a table for protocol and action. The 'Associated Profiles' list on the left shows the hierarchy of profiles associated with the configuration group.</p>
<b>Cisco Catalyst SD-WAN Monitor and Maintain</b>	
<a href="#">Device Information</a>	The <b>Monitor &gt; Devices</b> page displays the devices that are newly added or synced to Cisco SD-WAN Manager using the options available on the <b>Configuration &gt; Devices</b> page.
<b>Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)</b>	
<a href="#">Migrate a BGP-Based Hierarchical Core Network to Multi-Region Fabric</a>	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.
<b>Cisco Catalyst SD-WAN Getting Started Guide</b>	
<a href="#">Manage HSEC Licenses</a>	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
<b>Cisco Catalyst SD-WAN Getting Started</b>	

Feature	Description
<a href="#">Support for License Management Using a Proxy Server</a>	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.
<a href="#">Support for Managing Licenses Using Cisco Smart Software Manager On-Prem</a>	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.
<a href="#">Renew Device CSR</a>	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.
<a href="#">Support for Software Maintenance Upgrade Package</a>	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.
<b>Cisco Catalyst SD-WAN Systems and Interfaces</b>	
<a href="#">Hardened Passwords</a>	This feature lets you configure Cisco SD-WAN Manager to enforce predefined medium-security or high-security password criteria.

Feature	Description
<a href="#">Configuration Groups and Feature Profiles (Phase II)</a>	<p>The following enhancements are introduced for the Configuration Group feature.</p> <ul style="list-style-type: none"> <li>• Adds support for the following features: <ul style="list-style-type: none"> <li>• SNMP</li> <li>• Cellular Interface</li> <li>• BGP Routing (transport and management profile)</li> <li>• Wireless LAN</li> <li>• Switch Port</li> <li>• SVI Interface</li> <li>• DHCP Server</li> <li>• ThousandEyes</li> </ul> </li> <li>• Adds the IPv6 configuration support in the VPN, interface, and BGP features.</li> <li>• Adds the following options to the Global settings, which are a part of the system profile. These options have been added to the <b>Other Settings</b> tab. <ul style="list-style-type: none"> <li>• Generate keepalive timers when incoming or outgoing network connections are idle</li> <li>• Enable small TCP and UDP servers</li> <li>• Enable console logging</li> <li>• Enable IP source routing</li> <li>• Display log messages to a vty session</li> <li>• Enable SNMP IFINDEX persistence</li> <li>• Enable BOOTP server</li> </ul> </li> </ul>
<a href="#">Create Configuration Group Workflow for a Single-Router Site</a>	<p>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.</p>
<a href="#">Network Hierarchy and Resource Management</a>	<p>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.</p> <p>You can create a region only if you enable the <b>Multi-Region Fabric</b> option in Cisco SD-WAN Manager.</p>



Feature	Description
Wireless Management on Cisco 1000 Series Integrated Services Routers supporting WIFI6 WLAN module	<p>This feature enables you to configure the wireless LAN settings on WiFi6-capable Cisco 1000 Series Integrated Services Routers using Cisco SD-WAN Manager.</p> <p>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.</p>
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	<p>This feature provides the following default user groups:</p> <ul style="list-style-type: none"> <li>• network_operations user group for non-security policies</li> <li>• security_operations user group for security policies</li> </ul> <p>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.</p>
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.
<b>Cisco Catalyst SD-WAN Routing</b>	
Route Leaking between Inter-Service VPN	<p>This feature allows you to leak routes between service VPNs on the same edge device.</p> <p>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.</p>
<b>Cisco Catalyst SD-WAN Policies</b>	
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
<a href="#">Support for Cisco SD-WAN Policy Configuration Tagging Using the Cisco vSmart Controller CLI Template</a>	<p>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:</p> <ul style="list-style-type: none"> <li>Controls the policy configuration download speed between the Cisco SD-WAN Controller and the Cisco IOS XE Catalyst SD-WAN devices.</li> <li>Improves management of the defined lists in the Cisco vSmart Controller.</li> <li>Better organizes the configurations of the intent-based network.</li> </ul>
<a href="#">Lawful Intercept</a>	<p>This feature enhances the support for Lawful Intercept in Cisco Catalyst SD-WAN.</p> <p>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.</p>
<b>Cisco Catalyst SD-WAN Security</b>	
<a href="#">Cisco SD-WAN Identity-Based Firewall Policy</a>	<p>This feature allows you to configure user-identity-based firewall policies for unified security policies.</p> <p>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.</p>
<a href="#">Automatic GRE Tunnels to Zscaler</a>	<p>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.</p>
<a href="#">Global SIG Credentials Template</a>	<p>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 Manager SIG template to a device template, Cisco SD-WAN Manager automatically attaches the applicable global Cisco SIG Credentials template to the device template.</p>
<a href="#">Monitor Automatic SIG Tunnel Status and Events</a>	<p>Monitor security events related to automatic SIG tunnels using the <b>Security Events</b> pane on the <b>Monitor &gt; Security</b> page, and the <b>Events</b> dashboard on the <b>Monitor &gt; Logs</b> page.</p> <p>Monitor automatic SIG tunnel status using the <b>SIG Tunnel Status</b> pane on the <b>Monitor &gt; Security</b> page, and the <b>SIG Tunnels</b> dashboard on the <b>Monitor &gt; Tunnels</b> page.</p>
<a href="#">Disable Weak SSH Encryption Algorithms</a>	<p>This feature allows you to disable weaker SSH algorithms that may not comply with certain data security standards.</p>
<b>Cisco Catalyst SD-WAN Cloud OnRamp</b>	

Feature	Description
<a href="#">Improved Visibility for Microsoft 365 Traffic</a>	This feature provides improved visibility to allow you to monitor the details of Microsoft 365 traffic processed by Cloud OnRamp for SaaS.
<a href="#">Configure the Traffic Category and Service Area for Specific Policies</a>	You can edit AAR policies individually to change the specified Microsoft 365 traffic category and service area for specific AAR policies.
<a href="#">Enable Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites</a>	This feature allows you to selectively delete AAR policy sequences to exclude Cloud OnRamp for SaaS operation on specific applications at specific sites.
<a href="#">Option to Include or Exclude Microsoft Telemetry Data from Best Path Decision for Microsoft 365 Traffic</a>	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.
<a href="#">Support for AWS GovCloud (US) with Cisco SD-WAN Cloud OnRamp for Multicloud</a>	<p>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.</p> <p>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).</p>
<a href="#">Support for the Azure for US Government Cloud with Cisco SD-WAN Cloud OnRamp for Multicloud</a>	<p>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.</p> <p>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.</p>
<a href="#">Encrypted Multicloud Interconnects with Megaport</a>	You can extend the SD-WAN fabric from the Interconnect gateway in Megaport into the AWS, Google Cloud and Microsoft Azure Cloud Service Providers.
<a href="#">Encrypted Multicloud Interconnects with Equinix</a>	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
<a href="#">License Management for Cisco SD-WAN Cloud Interconnect with Megaport</a>	<p>To create Interconnect Gateways and Interconnect Connections in the Megaport fabric, you must purchase required licenses on Cisco Commerce Workspace.</p> <p>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.</p>
<a href="#">Decoupled Site-to-Site and Site-to-Cloud Connectivity Configuration for Cloud Gateways</a>	<p>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.</p> <p>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.</p>
<a href="#">Horizontal Scaling of Cisco Catalyst 8000V Instances in a Cloud Gateway</a>	<p>With this feature, you can deploy between two and eight Cisco Catalyst 8000V instances as part of a cloud gateway in a particular region.</p> <p>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.</p>
<b>Cisco Catalyst SD-WAN AppQoE</b>	
<a href="#">HTTP Connect</a>	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.
<b>Cisco SD-WAN Monitor and Maintain</b>	
<a href="#">Access TAC Cases from Cisco SD-WAN Manager</a>	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.
<a href="#">Analyze the Health of the Cisco SD-WAN Manager Cluster and Cluster Services Using the CLI</a>	With this feature, you can analyze the health of the Cisco SD-WAN Manager cluster and the status of the cluster services using the <b>request nms cluster diagnostics</b> CLI command.
<a href="#">Additional Real Time Monitoring Support for AppQoE and Other Configuration Options</a>	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 <b>show</b> commands in the CLI of a device.
<a href="#">Customizable Monitor Overview Dashboard in Cisco SD-WAN Manager</a>	This feature adds customizability to the <b>Monitor Overview</b> 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 <b>Config Diff</b> option for audit logs of device templates and feature templates. The <b>Config Diff</b> option shows configuration changes made to the template, comparing the current configuration and previous configuration.  The <b>Config Diff</b> 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.
<b>Cisco Catalyst SD-WAN NAT</b>	
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
<a href="#">Support for Port Forwarding with NAT DIA</a>	<p>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.</p> <p>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.</p>
<a href="#">Support for NAT High-Speed Logging</a>	<p>This feature provides the ability to enable or disable high-speed logging (HSL) of all translations by NAT.</p> <p>The new <b>ip nat log translations flow-export</b> command is introduced.</p> <p>You can configure NAT HSL using a device CLI or a CLI add-on template.</p>
<b>Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)</b>	
<a href="#">Re-Origination Dampening</a>	<p>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.</p> <p>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.</p>
<a href="#">Migrating to Multi-Region Fabric</a>	<p>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.</p> <p>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.</p>
<a href="#">Match Traffic by Destination Region</a>	<p>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.</p>
<a href="#">Specify Path Type Preference</a>	<p>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.</p>
<b>High Availability</b>	
<a href="#">Configure Disaster Recovery Alerts</a>	<p>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.</p>



## 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

*Table 4: 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 devices and Cisco Catalyst SD-WAN overlay do not require the Organizational Unit field. However, if a signed certificate includes the Organizational Unit field, the organization name configured on the device. This is described in the <a href="#">Configure Enterprise Certificates</a> section.

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

*Table 5: Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.9.2a*

Behavior Change	Description
A <b>show sdwan from-vsmart commit-history</b> command is added for verifying policy-related commit events and for analyzing the average time required for the policy commit.	A new command, <a href="#">show sdwan from-vsmart commit-history</a> .
The <b>snmp-server subagent fetch count</b> 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 <a href="#">Supported SNMP MIBs</a> section.

Behavior Change	Description
The <b>Community Name</b> field has been removed from the SNMP feature. In its place, the <b>User Label</b> 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 <b>User Label</b> field is described in the <a href="#">SNMP</a> section. The <b>Community Name</b> field.
An <b>Internet Outages</b> option is added to the <b>Analytics</b> menu in Cisco SD-WAN Manager.	The <b>Internet Outages</b> option is described in the <a href="#">Internet Outages</a> section.

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

**Table 6: 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 <a href="#">Configure TCP MSS and Clear Dont F</a> section. A note is added in the <a href="#">Information About Using a Dialer Inter</a> section.
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 <b>SD-WAN Portal</b> 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 <a href="#">Cisco Catalyst SD-WAN Solution</a> section.
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 <a href="#">Configure Device Access Policy Using</a> section.
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 <a href="#">Upgrade the Software Image on a Dev</a> section.
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 <a href="#">Configure the Cisco vSmart Controller</a> section.
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 <a href="#">Configure PPPoE using Cisco vManag</a> section.



Behavior Change	Description
Support is added to manually enable or disable the unified logging fields in flexible netflow (FNF) using the <b>policy ip visibility features enable</b> command.	A note is added in the <a href="#">Unified Logging Security Connect Troubleshooting</a> sections. A new command <b>policy ip visibility features enable</b> is added.
The <b>show sdwan omp routes</b> command now includes <b>tenant-id</b> and <b>verify</b> keywords.	The <b>show sdwan omp routes</b> 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 <a href="#">Guidelines for a Cisco vManage Cluster</a> section.
With the <b>Enable telemetry pull from and push to Microsoft</b> 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 <a href="#">Enable Application Feedback Metrics</a> section.
A new option <b>Traffic Steering</b> 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 <b>Traffic Steering</b> is updated in the <a href="#">Enable Office 365 Traffic</a> section.
A new option <b>Umbrella DNS Certificate</b> is available in Cisco SD-WAN Manager to upload and push to appropriate devices Umbrella root certificates for Umbrella DNS security.	The new <b>Umbrella DNS Certificate</b> option is described in the <a href="#">Certificates</a> section.
The IP address of an NTP server cannot be a broadcast or a multicast address.	A note is added in the <a href="#">Configure NTP</a> 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 <a href="#">Restrictions for Managing Licenses Policy</a> section.
Use the <b>implicit-acl-on-bind-intf</b> 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 <b>Loopback TLOC Interface Bound</b> section in <a href="#">Information About Implicit ACL on Loopback</a> section.
The Cisco SD-WAN Controller software version must be the same or be higher than 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 <a href="#">Cisco SD-WAN Controller Compatibility Computing Resources</a> .

Behavior Change	Description
<p>Use the new tags for authentication and accounting.</p> <ul style="list-style-type: none"> <li>• Viptela-User-Group: for user group definitions instead of Viptela-Group-Name</li> <li>• Viptela-Resource-Group: for resource group definitions.</li> </ul>	<p>A note is added in the <a href="#">Configure the Authentication Order</a>.</p>

## 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.

- Hardened security posture

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.

- Keyword for commands with output in tabular format

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.

- Feature template support for network interface modules

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)

- Switch Port feature template

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.

- Route-target CLIs

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
```

- Minimum supported release for software maintenance upgrade (SMU)

The minimum supported release for software maintenance upgrade is Cisco IOS XE Catalyst SD-WAN Release 17.9.5a. It was previously described as Cisco IOS XE Catalyst SD-WAN Release 17.9.1a. See [Supported Devices for Software Maintenance Upgrade](#).

## 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 17.9.7b

#### Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.7b

Identifier	Headline
<a href="#">CSCwo25107</a>	Cisco IOS XE Catalyst SD-WAN devices running 17.12.4 crashes due to memory pressure exceeding threshold.
<a href="#">CSCwp01534</a>	Elevated memory usage on Cisco ISR1100-4G/6G devices.

### Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.7a

#### Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.7a

Identifier	Headline
<a href="#">CSCwn53881</a>	Rekeying does not work for the PWK and Non-PWK interworking use case.
<a href="#">CSCwn49931</a>	The FMAN_FP crashes while running longevity traffic with triggers.
<a href="#">CSCwm61871</a>	SLA-Change events incorrectly display "None" for both old-sla and new-sla values.
<a href="#">CSCwi74743</a>	[SITLite]Observing BFD down issue between Cisco IOS XE Catalyst SD-WAN device boxes.
<a href="#">CSCwi61369</a>	Cisco IOS XE Catalyst SD-WAN device device may unexpectedly reload due to SIGABRT.

Identifier	Headline
<a href="#">CSCwk16333</a>	Cisco IOS XE Catalyst SD-WAN deviceRepeated crashes in FTMD due to FNF flow additions.
<a href="#">CSCwj95633</a>	In the SDWAN SAIE application, no data is displayed over Cisco SD-WAN Manager for IOS XE routers.
<a href="#">CSCwf89408</a>	Cisco IOS XE Catalyst SD-WAN device undergoes an unexpected reload due to the ftmd process following a TLOC flap.
<a href="#">CSCwm28775</a>	An update to the certificate (ios_core.p7b bundle) is required for Umbrella DNS using the TOKEN method on versions 17.6, 17.9, and 17.12.
<a href="#">CSCwm63773</a>	Cisco IOS XE Catalyst SD-WAN device A crash occurs with the critical process vip_confid_startup_sh fault due to a large number of zbfw-dp sessions.
<a href="#">CSCwm46805</a>	IPSec auto AR recovery.
<a href="#">CSCwn40906</a>	A router crash is observed when optimizing encrypted traffic using DRE
<a href="#">CSCwm53179</a>	BFD flaps reset the Tunnel MTU to the configured value, and subsequent PMTU (Path MTU) discovery is ignored.
<a href="#">CSCwn52348</a>	Removing and re-adding NAT causes BFD to go down intermittently.
<a href="#">CSCwi71474</a>	cEdge_sdwan_smu API based SMU install is not working in 20.14.1
<a href="#">CSCwe92757</a>	Excessive btrace logs from the fman_rp/sdwan-overlay feature are impacting log retention.
<a href="#">CSCwn27896</a>	Device crashed at FTMD process.
<a href="#">CSCwn81320</a>	The confd_cli processes show high CPU usage & hangs when executing show sdwan ftm CLI commands at scale.
<a href="#">CSCwm02750</a>	Implement TLOC tracing for IPsec ADD/DEL
<a href="#">CSCwm73365</a>	The SSL handshake fails even though the device has the latest umbrella_root_ca.ca certificate installed.
<a href="#">CSCwk70415</a>	An unexpected reload occurs due to a stuck thread in IOS-XE with NAT BPA configuration.
<a href="#">CSCwm61553</a>	Cisco IOS XE Catalyst SD-WAN device unexpected relaod due to NAT logging buffer management.
<a href="#">CSCwh65016</a>	Unexpected Reboots on Cisco IOS XE Catalyst SD-WAN device due to QFP exception.
<a href="#">CSCwm48459</a>	Software crash with Critical process vip_confid_startup_sh fault on rp_0_0 (rc=6)
<a href="#">CSCwm61790</a>	SDWAN BFD does not start the bfd detection timer on BFD_INIT state.
<a href="#">CSCwn39963</a>	NAT DIA packets are randomly dropped due to Ipv4RoutingErr
<a href="#">CSCwk90014</a>	NAT DIA traffic is getting dropped due to port allocation failure.

Identifier	Headline
<a href="#">CSCwm37504</a>	vManaged Cisco IOS XE Catalyst SD-WAN device Upgrade 17.3.3 to 17.9.5a removes OMP service side VRF address-family configuration.
<a href="#">CSCwd37700</a>	Cisco IOS XE Catalyst SD-WAN device router crashed under scale when clear BFD sessions with show sdwan session.
<a href="#">CSCwj87028</a>	The cflowd showing custom APP as "unknown" for egress traffic when using DRE Opt.
<a href="#">CSCwk08216</a>	FW dropping VPN traffic even after zone-pair policy is removed.
<a href="#">CSCwi60266</a>	After an upgrade, a Cisco IOS XE Catalyst SD-WAN device with enterprise certificates fails to form control connections with controllers.
<a href="#">CSCwn35075</a>	Cisco IOS XE Catalyst SD-WAN device Unexpected reload after Overlay Session delete while deleting AVL tree.
<a href="#">CSCwn37784</a>	The fman-fp cce-class-grp memory leak with per-tunnel qos policy when BFD session flaps.

#### Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.7a

Identifier	Headline
<a href="#">CSCwd90056</a>	C8500-12X4QC P2MP WAN MACSEC does not allow traffic to pass on the link.
<a href="#">CSCwh94444</a>	The post-upgrade checks didn't detect a weak crypto configuration command esp-null leading to network outage.
<a href="#">CSCwb74821</a>	Cisco IOS XE Catalyst SD-WAN device: Unexpected behavior due to unstable power source.
<a href="#">CSCwm72748</a>	Crash in OMPd process: Crashes occur due to a SIGABRT signal when the pthread limit is reached.

### Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.6

#### Resolved Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.6

Identifier	Headline
<a href="#">CSCwd31983</a>	[17.9-17.11] C1111-8P Inventory mismatch is seen after upgrading to 17.11
<a href="#">CSCwj59970</a>	Some duplicated packets are dropped when there are frequent BFD flaps on primary path transport.
<a href="#">CSCwi83365</a>	C1117-4PLTEEA platform crashed with sh pl hard qfp ac feat cef-mpls prefix ip 10.40.201.10/32 vrf 2
<a href="#">CSCwi43360</a>	Certificate expiry on Sept 2024 for DNS Security registration to Umbrella cloud.

Identifier	Headline
<a href="#">CSCwk42634</a>	%PMAN-0-PROCFAILCRIT: R0/0: pvp: A critical process vip_confid_startup_sh has failed (rc 6)
<a href="#">CSCwh84068</a>	Cisco Catalyst 8000V Edge router crash after changing NAT HSL configuration.
<a href="#">CSCwf43470</a>	Cisco IOS XE Catalyst SD-WAN device : Traceroute not working with NAT pool configuration.
<a href="#">CSCwk39131</a>	Cisco IOS XE Catalyst SD-WAN device crashed when issuing "show sdwan ftm next-hop chain all" .
<a href="#">CSCwj14121</a>	The snmpwalk for OID ifOperStatus gives different output before & after upgrade for serial interface.
<a href="#">CSCwi31523</a>	EPBR FIA is not enabled on port-channel sub-interface.
<a href="#">CSCwk39391</a>	Multicast drops seen due to IpsecOutput drops - OUT_IPV4_SA_NOT_FOUND.
<a href="#">CSCwj80904</a>	Crash on Cisco 1000 Series Integrated Services Routers (double free or corruption).
<a href="#">CSCwi33634</a>	Cisco IOS XE Catalyst SD-WAN device is incorrectly consuming icmp reply packets.
<a href="#">CSCwj25493</a>	Cisco IOS XE Catalyst SD-WAN device crashed twice with critical process linux_iosd_image fault on rp_0_0
<a href="#">CSCwi05395</a>	The snmpbulkget cannot get loss, latency and jitter for ProbeClassTable & ClassIntervalTable OIDs.
<a href="#">CSCwj45177</a>	"dmidecode: command not found" error seen executing "show sdwan certificate validity"
<a href="#">CSCwj27545</a>	Cisco IOS XE Catalyst SD-WAN device router crashing due to ftmd.
<a href="#">CSCwj90614</a>	High CPU utilisation for confd_cli
<a href="#">CSCwi91887</a>	IPsec PWK SPI mismatch causes Cisco IOS XE Catalyst SD-WAN device bfd tunnels to remain in down state.
<a href="#">CSCwh39906</a>	Cisco IOS XE Catalyst SD-WAN device: confd_cli may cause high cpu. Parent PID of "confd_cli" containing "show ip fib".
<a href="#">CSCwj76662</a>	Cisco IOS XE Catalyst SD-WAN device - High memory utilization due to "ftmd" process.
<a href="#">CSCwi59854</a>	The 'show sdwan policy service-path' command gives inconsistent results with app name specified.
<a href="#">CSCwi46413</a>	Cisco IOS XE Catalyst SD-WAN device does not install OMP route with high preference using service chaning.
<a href="#">CSCwi32044</a>	Cisco IOS XE Catalyst SD-WAN device might reboot due to vip_config_startup_sh process failure.
<a href="#">CSCwi89822</a>	Unexpected reboot due cpp ucode on a Cisco Catalyst 8000V Edge router.

Identifier	Headline
<a href="#">CSCwk19970</a>	Cisco IOS XE Catalyst SD-WAN device URLF is unable to detect TLS SNI with "TLS1.3 hybridized Kyber support" enabled on the browser.
<a href="#">CSCwe10747</a>	The cxpd crash seen on IOS-XE platform.
<a href="#">CSCwj42249</a>	Disabling PMTU-Discovery with MTU change and BFD flap breaks packet duplication.
<a href="#">CSCwj24698</a>	The VFR enablement difference with NAT interface vs NAT pool configuration.
<a href="#">CSCwi44633</a>	Fragmented Radius Access-Request packets are dropped when NWPI is running.
<a href="#">CSCwj58176</a>	Cisco IOS XE Catalyst SD-WAN device performing NAT for directly connected traffic.
<a href="#">CSCwh99399</a>	The ftmd crash observed while running PWK suite.
<a href="#">CSCwh82168</a>	One of IPSEC IKE tunnel goes down when second IPSEC IKE tunnel has been shut with same source interface.
<a href="#">CSCwk19725</a>	Add FNF cache limit for show sdwan app-fwd flows for CSCwj02401.
<a href="#">CSCwi16015</a>	[SIT]: SSE tunnels don't come up with Dialer interface. Relax check in IKE.
<a href="#">CSCwf89860</a>	20.12-ISR4431 ftmd crash @sig while removing IPv6 DNS server configuration.
<a href="#">CSCwf98902</a>	Cisco IOS XE Catalyst SD-WAN device: Unexpected reboot fman_fp_image fault on fp_0_0 (rc=134).
<a href="#">CSCwj49941</a>	The dns-snoop-agent has TCAM entry with all zeros for some regex patterns.
<a href="#">CSCwi78940</a>	The snmpbulkget/snmpwalk can't get loss latency jitter for ProbeClassTable & ClassIntervalTable OIDs.

#### Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.6

Identifier	Headline
<a href="#">CSCwh72441</a>	The show sdwan appqoe aoim-statistics - APPQOE services restart.
<a href="#">CSCwi61369</a>	Cisco IOS XE Catalyst SD-WAN device may unexpectedly reload due to SIGABRT.
<a href="#">CSCwe35574</a>	DPDK RX buffer is getting corrupted on both Radium and Fugazi and causing crash.
<a href="#">CSCwb74821</a>	Cisco IOS XE Catalyst SD-WAN device: Unexpected behavior due to unstable power source.
<a href="#">CSCwj01917</a>	After Upgrade to 17.9.4a, Cellular Interface IP ADDRESS NEGOTIATED Mismatching.
<a href="#">CSCwm27495</a>	OMP route is being advertised although the route is not available (network statement + NAT DIA VPN).

Identifier	Headline
<a href="#">CSCwm28775</a>	Certificate (ios_core.p7b bundle) update required for umbrella DNS for TOKEN method on 17.6/9/.12
<a href="#">CSCwf51886</a>	Cisco IOS XE Catalyst SD-WAN device: sh sdwan omp routes 0.0.0.0/0 vpn 1 throws CLI error.
<a href="#">CSCwh63864</a>	Service-side NAT Translation discrepancy.
<a href="#">CSCwf40849</a>	Cisco IOS XE Catalyst SD-WAN device IPv6: removing "advertise aggregate" configuration does not remove the entry from OMP.
<a href="#">CSCwm28826</a>	Cisco IOS XE Catalyst SD-WAN device unable to establish Cisco SD-WAN Validator connection on a cellular interface.
<a href="#">CSCwf44703</a>	Cisco IOS XE Catalyst SD-WAN device: NAT64 prefix is not originated into OMP.
<a href="#">CSCwm27478</a>	IOS-XE SDWAN: Warning Message when customer configures allow-service all.
<a href="#">CSCwd44167</a>	SPA_SETUP_FAILURE traceback seen after a reboot.
<a href="#">CSCwk42817</a>	In snmpbulkwalk request on Cisco IOS XE Catalyst SD-WAN device, each snmp get bulk retrieves data from backend instead of cache.
<a href="#">CSCwh65016</a>	Unexpected reboots on Cisco IOS XE Catalyst SD-WAN device due to QFP exception.
<a href="#">CSCwi51381</a>	TrapOID of ciscoSdwanBfdStateChange is different from MIB file.
<a href="#">CSCwk38020</a>	AAR BOW is not choosing the best tunnel; it is load balancing among the tunnels.
<a href="#">CSCwj99827</a>	Cisco IOS XE Catalyst SD-WAN device unexpectedly reloads due to a crash in 'vdaemon' process.
<a href="#">CSCwm29499</a>	Cisco IOS XE Catalyst SD-WAN device advertises component routes temporarily even if omp aggregate-only is configured.
<a href="#">CSCwk90014</a>	NAT DIA traffic getting dropped due to port allocation failure.
<a href="#">CSCwm27749</a>	Speed test download issue on C8200 platform seen with IPSEC Zscaler.
<a href="#">CSCwm07994</a>	Router crash with stuck threads.
<a href="#">CSCwi60266</a>	Cisco IOS XE Catalyst SD-WAN device with enterprise certificates not forming control connections with controllers after upgrade.
<a href="#">CSCwm08545</a>	Centralized Policy Policer worked per PC on the same site not per site/vpn-list.
<a href="#">CSCwm11348</a>	Enpoint tracker reporting error due to "DNS Query Error".
<a href="#">CSCwf45486</a>	OMP to BGP Redistribution Leads to Incorrect AS_Path Installation on Chosen Next-Hop.
<a href="#">CSCwf62943</a>	Cisco IOS XE Catalyst SD-WAN device: System image file is not set to packages.conf when image expansion fails due to disk space.



## Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.5f

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

Identifier	Headline
<a href="#">CSCwh70484</a>	Per-tunnel QoS convergence slows down when the number of policy-map instances increases.
<a href="#">CSCwi49363</a>	The confd_cli processes is hanging and reaching maximum CPU usage.
<a href="#">CSCwn52348</a>	Remove and re-add NAT causes BFD to go down (Intermittent).
<a href="#">CSCwn81320</a>	The confd_cli processes hang and exhibit high CPU usage when executing show sdwan ftm CLI commands at scale.

## Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.5e

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

Identifier	Headline
<a href="#">CSCwi91887</a>	IPsec PWK SPI mismatch causes Cisco IOS XE Catalyst SD-WAN device bfd tunnels to remain in down state.
<a href="#">CSCwf74216</a>	After applying security ipsec integrity-type Cisco IOS XE Catalyst SD-WAN device not recover BFD with CD_IN_PKT_OUT_OF_WINDOW drop.
<a href="#">CSCwh39906</a>	Cisco IOS XE Catalyst SD-WAN device : confd_cli may cause high cpu. Parent PID of "confd_cli" containing "show ip fib".
<a href="#">CSCwh99399</a>	The ftmd crash observed while running PWK suite.
<a href="#">CSCwi74743</a>	[SITLite]Observing BFD down issue between Cisco IOS XE Catalyst SD-WAN device boxes.
<a href="#">CSCwj74769</a>	After pairwise key enabling and reboot, there is a bfd mismatch on device.
<a href="#">CSCwk19725</a>	The add FNF cache limit for show sdwan app-fwd flows for CSCwj02401.
<a href="#">CSCwn20614</a>	17.17.1 After change integrity-type twice, all bfd sessions will be down.
<a href="#">CSCwk87944</a>	VRRP switchover with TLOC preference change is generating rekey and crypto add/delete events.
<a href="#">CSCwf98902</a>	Cisco IOS XE Catalyst SD-WAN device: Unexpected reboot fman_fp_image fault on fp_0_0 (rc=134)
<a href="#">CSCwf89408</a>	Cisco IOS XE Catalyst SD-WAN device unexpected reload due to ftmd process after tloc flap
<a href="#">CSCwm48459</a>	Software crash with Critical process vip_confid_startup_sh fault on rp_0_0 (rc=6)

Identifier	Headline
<a href="#">CSCwk39131</a>	Cisco IOS XE Catalyst SD-WAN device crashed when issuing "show sdwan ftm next-hop chain all".
<a href="#">CSCwm78086</a>	The BFD session went down after changing the TLOC preference with pairwise-keying enabled.

## Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.9.5a

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

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

Identifier	Headline
<a href="#">CSCwb74384</a>	Cisco IOS XE Catalyst SD-WAN device: confd_cli high CPU utilization after executing "show sdwan app-route stats".
<a href="#">CSCwf21973</a>	Device replying with NAT pool IP address instead of the WAN IP address.
<a href="#">CSCwh70449</a>	PMTUD incorrectly converging without attempting to learn a higher MTU.
<a href="#">CSCwf95095</a>	Intermittent BFD session flaps on Cisco IOS XE Catalyst SD-WAN device service side interface .
<a href="#">CSCwf25249</a>	The AppQoS DRE shows the optimized traffic is more than the original traffic on the data center SCs.
<a href="#">CSCwf65799</a>	There is fpm crash on device after Power ON when trying to sync the config.
<a href="#">CSCwh29805</a>	The custom-app based policy triggering protocol deactivation and cpp traceback with traffic failure
<a href="#">CSCwi27324</a>	Tunnels behind Sym-nat does not come up or flap after "clear omp all" trigger on HUB.
<a href="#">CSCwe83353</a>	17.10: PPPoA dialer doesnt come up and randomly test case are failing when ran 174_aldi_script.
<a href="#">CSCwd20182</a>	[SIT]:When firewall is enabled , speedtest with iperf server configured on vpn 0 fails.
<a href="#">CSCwe49684</a>	Cisco Catalyst SD-WAN BFD sessions keeps flapping intermittently.
<a href="#">CSCwf71051</a>	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 17.9.5a

Identifier	Headline
<a href="#">CSCwd31983</a>	[17.9-17.11] C1111-8P Inventory mismatch is seen after upgrading to 17.11.
<a href="#">CSCwh72441</a>	The show sdwan appqoe aoim-statistics - APPQOE services restart
<a href="#">CSCwb74821</a>	Cisco IOS XE Catalyst SD-WAN device: unexpected behavior due to unstable power source.
<a href="#">CSCwh94444</a>	Post-upgrade checks didn't detected weak crypto config command esp-null leading to network outage.
<a href="#">CSCwi31523</a>	EPBR FIA is not enabled on Port-channel sub-interface.
<a href="#">CSCwh63864</a>	Service-side NAT Translation discrepancy
<a href="#">CSCwe86434</a>	Static NAT DIA inside static routes being advertised over OMP to remote sites.
<a href="#">CSCwf40849</a>	Cisco IOS XE Catalyst SD-WAN device IPv6: removing "advertise aggregate" configuration does not remove the entry from OMP.

Identifier	Headline
<a href="#">CSCwd97769</a>	Encryption supported still shows AES_256_CBC in security info of Cisco IOS XE Catalyst SD-WAN device.
<a href="#">CSCwa19332</a>	Fragmeneted packets getting dropped unexpectedly when second fragment packet no translate.
<a href="#">CSCwf44703</a>	Cisco IOS XE Catalyst SD-WAN device: NAT64 prefix is not originated into OMP
<a href="#">CSCwi07137</a>	Crash when traffic is sent to UTD
<a href="#">CSCwi58561</a>	Cisco IOS XE Catalyst SD-WAN Device : Tracker not working after software upgrade
<a href="#">CSCwf73123</a>	BFD timers reverting back to default value after negotiating correctly
<a href="#">CSCwh39906</a>	Cisco IOS XE Catalyst SD-WAN device: confd_cli may cause high cpu. Parent PID of "confd_cli" containing "show ip fib"
<a href="#">CSCwi59854</a>	'show sdwan policy service-path' command gives inconsistent results with app name specified.
<a href="#">CSCwh65016</a>	Unexpected Reboots on Cisco IOS XE Catalyst SD-WAN device due to QFP exception
<a href="#">CSCwi51381</a>	TrapOID of ciscoSdwanBfdStateChange is different from MIB file.
<a href="#">CSCwi32044</a>	Device reboot due to "Critical process vip_confid_startup_sh"
<a href="#">CSCwi15688</a>	Unexpected NAT translation occurs in a specific network.
<a href="#">CSCwe25926</a>	Tracker group is down if one of the tracker elements is not reachable.
<a href="#">CSCwi60266</a>	Cisco IOS XE Catalyst SD-WAN device with enterprise certificates not forming control connections with controllers after upgrade
<a href="#">CSCwi62230</a>	SIG tunnel: 'SIG STATE' is showing blank value.
<a href="#">CSCwe64991</a>	Cisco SD-WAN Manager is reporting abnormal latency & jitter parameters
<a href="#">CSCwi19875</a>	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
<a href="#">CSCwh87343</a>	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
<a href="#">CSCwd45508</a>	Cisco IOS XE Catalyst SD-WAN device does not form BFD across Serial link when upgrading from 17.3.3 to 17.6.x
<a href="#">CSCwd41236</a>	On C8200-1N-4T, sh version points to /harddisk/core dir, but file is present in /bootflash/core dir
<a href="#">CSCwe93905</a>	NAT ALG is changing the Call-ID within SIP message header causing calls to fail
<a href="#">CSCwe28204</a>	Catalyst 8500L: Control connection over L3 Tloc extension failing as no NAT table entry created
<a href="#">CSCwe43341</a>	TLS control-connections down, traffic from controller dropped with SdwanImplicitAclDrop
<a href="#">CSCwe18276</a>	17.6: Route-map not getting effect when its applied in OMP for BGP routes
<a href="#">CSCwf38166</a>	CPP Ucode crash when Multicast traffic and UTD is enabled together on the same Cisco IOS XE Catalyst SD-WAN device
<a href="#">CSCwe69572</a>	Zscaler SIG: Tunnels don't come up with Custom Data Center IP
<a href="#">CSCwd87195</a>	NAT configuration with redundancy, mapping id and match-in-vrf options with no-alias support.
<a href="#">CSCwe58264</a>	TLOC down post ios-xe to viptela Nutella migration when enterprise cert used
<a href="#">CSCwd34941</a>	NAT configuration with no-alias option is not preserved after reload
<a href="#">CSCwe81991</a>	fugazi crash with qfp-ucode-fugazi in C8500L at @posix_mempool_prime_cache
<a href="#">CSCwe23276</a>	Change in the IPsec integrity parameters breaks the connectivity
<a href="#">CSCwd49309</a>	17.10: ucode crash seen on Thorium with traffic pointing to segfault in coff handler
<a href="#">CSCwe31471</a>	Segmentation fault in SDWAN PB rx when per-tunnel qos config withdraw
<a href="#">CSCwe49009</a>	Cisco IOS XE Catalyst SD-WAN device Router Crashes in "ftmd" Process When Configuring Tunnel "mode" or "route-via"
<a href="#">CSCwe70374</a>	c8300/85000 platform punt-policer is not configurable
<a href="#">CSCwe18058</a>	Unexpected reload with IPS configured on 17.6.3a
<a href="#">CSCwe73653</a>	Cisco IOS XE Catalyst SD-WAN device router crashing due to memory leak in ftmd
<a href="#">CSCwd66293</a>	Traffic blackhole seen after few hrs of soak due to Extra Key
<a href="#">CSCwe85421</a>	Cisco IOS XE Catalyst SD-WAN device BFD Session Down with interface flap
<a href="#">CSCwd81262</a>	Restrict option does not work when traffic match both Data policy and AAR policy

Identifier	Headline
<a href="#">CSCwe15537</a>	Cisco IOS XE Catalyst SD-WAN device:After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.
<a href="#">CSCvy23366</a>	C8300-2N2S + UCSE: Kernel crash on C8300-2N2S with UCSE module.
<a href="#">CSCwe70642</a>	AAR overlay actions are applied to DIA traffic
<a href="#">CSCwe79007</a>	Cisco IOS XE Catalyst SD-WAN device unexpected reload when doing ips test with UTD ips engine
<a href="#">CSCwe09341</a>	TLOC down post viptela to ios-xe Nutella migration when enterprise cert used
<a href="#">CSCwf16608</a>	Cisco IOS XE Catalyst SD-WAN device configured with 10G BDI might reload when running NWPI Trace with QoS Insight enabled
<a href="#">CSCwf26771</a>	Invalid L4 Header drop due to multiple encap
<a href="#">CSCwd79572</a>	FW policy with app-family rule with FQDN causes traffic drop for other sequences
<a href="#">CSCwf37888</a>	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
<a href="#">CSCwf51144</a>	Zombie confd_cli processes hanging around are maxing out CPU
<a href="#">CSCwc86434</a>	Static NAT DIA inside static routes being advertised over OMP to remote sites
<a href="#">CSCwf40849</a>	Cisco IOS XE Catalyst SD-WAN device IPv6: removing "advertise aggregate" configuration does not remove the entry from OMP
<a href="#">CSCwd01378</a>	OMPD crash while withdrawing routes
<a href="#">CSCwc83353</a>	17.10: PPPoA dialer doesnt come up and randomly test case are failing when ran 174_aldi_script
<a href="#">CSCwd53710</a>	17.10 - Crash seen when umbrella/zscaler template pushed to device when name_lookup takes > 30 sec
<a href="#">CSCwf45486</a>	OMP to BGP Redistribution Leads to Incorrect AS_Path Installation on Chosen Next-Hop
<a href="#">CSCwf21973</a>	Device replying with NAT pool IP address instead of the WAN IP address
<a href="#">CSCwd97769</a>	Encryption supported still shows AES_256_CBC in security info of Cisco IOS XE Catalyst SD-WAN device
<a href="#">CSCwf44703</a>	Cisco IOS XE Catalyst SD-WAN device: NAT64 prefix is not originated into OMP
<a href="#">CSCwd20182</a>	[SIT]:When firewall is enabled , speedtest with iperf server configured on vpn 0 fails.

Identifier	Headline
<a href="#">CSCwf39945</a>	Device requested SLAC without customer issuing command
<a href="#">CSCwf35823</a>	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
<a href="#">CSCwc68069</a>	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature
<a href="#">CSCwc76082</a>	check_sig_ipsec_ike_sessions fails with could not find entry for Tunnel100001
<a href="#">CSCwe00946</a>	Cisco Catalyst SD-WAN   System crash after disabling endpoint-tracker on tunnel interfaces
<a href="#">CSCwc48427</a>	[SITLite] BFD issues with clear_omp -&gt; non-PWK + non-VRRP scenario only
<a href="#">CSCwd15560</a>	With 2 sequences, should not skip if the match is different and action is same
<a href="#">CSCwd71656</a>	17.10 Auto GRE- After reboot, no ip address assigned to destination address for 1 tunnel
<a href="#">CSCwd12955</a>	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured
<a href="#">CSCwd67198</a>	17.10: uCode crash seen on Curie 2RU after stopping NWPI trace
<a href="#">CSCwd47940</a>	Cisco IOS XE Catalyst SD-WAN device: PMTU Discovery is not working after interface flap
<a href="#">CSCwb32635</a>	17.6.2 IOS XE SD-WAN - tech files are incomplete when running admin-tech
<a href="#">CSCwe29430</a>	[SIT] ISR4221X/K9 : Critical process fpm fault on rp_0_0 (rc=134)
<a href="#">CSCwd34573</a>	Sparrow crashed: fman_fp_image: QFP0.0 CPP Driver LOCKDOWN encountered due to previous fatal error
<a href="#">CSCwd15070</a>	Cisco IOS XE Catalyst SD-WAN device upgrade fails and can't change template due to "advertise aggregate" config w/o prefix-list
<a href="#">CSCwc77003</a>	Prefix through hub not intalled in FIB, with OD Tunnels, seeing drops due to FirewallPolicy
<a href="#">CSCwe06507</a>	Cisco IOS XE Catalyst SD-WAN device drops packets with reason 55 (Forus) when port forwarding is enabled from outside to inside
<a href="#">CSCwd44006</a>	Control Connection on Cisco IOS XE Catalyst SD-WAN device doesn't come-up with reverse proxy using Enterprise Certificate

Identifier	Headline
<a href="#">CSCwd71586</a>	BFD sessions flapping on an interface with SYMNAT may lead to IPSec crash
<a href="#">CSCwd44439</a>	ASR and c8500 crashing at fman_sdwan_nh_indirect_delete_from_hash_table
<a href="#">CSCwd14061</a>	FTM is shooting up high and stuck in loop with the function ftm_sa_add().
<a href="#">CSCwd44586</a>	Cisco IOS XE Catalyst SD-WAN device - Login banner config is changed after upgrade to 17.6.3a
<a href="#">CSCwd01326</a>	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
<a href="#">CSCwd42523</a>	Same label is assigned to different VRFs
<a href="#">CSCwd45508</a>	Cisco IOS XE Catalyst SD-WAN device does not form BFD across Serial link when upgrading from 17.3.3 to 17.6.x
<a href="#">CSCwd76364</a>	Cisco IOS XE Catalyst SD-WAN device crash with imgr_n2_ipsec_sa_ctx_register
<a href="#">CSCwe23276</a>	Change in the IPsec integrity parameters breaks the connectivity
<a href="#">CSCwd97350</a>	Cisco IOS XE Catalyst SD-WAN device did not created a crash file after Critical software exception
<a href="#">CSCwe18058</a>	Unexpected reload with IPS configured on 17.6.3a
<a href="#">CSCwe28204</a>	Cisco Catalyst 8500L: Control connection over L3 Tloc extension failing as no NAT table entry created
<a href="#">CSCwd90056</a>	C8500-12X4QC P2MP WAN MACSEC does not allow traffic to pass on the link
<a href="#">CSCwe19394</a>	Cisco IOS XE Catalyst SD-WAN device: device may boot up into prev_packages.conf due to power outage
<a href="#">CSCwe27241</a>	nbar classification error with custom app-aware routing policy
<a href="#">CSCwd53710</a>	17.10 - Crash seen when umbrella/zscaler template pushed to device when name_lookup takes > 30 sec
<a href="#">CSCwe32140</a>	Nutella Cisco IOS XE Catalyst SD-WAN device do not accept the password via netconf
<a href="#">CSCwe09341</a>	TLOC down post vptela to ios-xe Nutella migration when enterprise cert used
<a href="#">CSCwd79572</a>	FW policy with app-family rule with FQDN causes traffic drop for other sequences
<a href="#">CSCwd10988</a>	Cisco IOS XE Catalyst SD-WAN device crashes due to OMP process
<a href="#">CSCvy53031</a>	Inconsistent behavior found when adding tunnel source config to virtual-template interface



Identifier	Headline
<a href="#">CSCwc24654</a>	Cisco IOS XE Catalyst SD-WAN device app-route Stats Show 100 percent loss but tunnel was up
<a href="#">CSCwd34941</a>	NAT configuration with no-alias option is not preserved after reload
<a href="#">CSCwd97774</a>	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
<a href="#">CSCwb65396</a>	C1116-4P: CLI template push fails with error: 'Error: on line 48: line-mode single-wire line 0'
<a href="#">CSCwc23077</a>	Firewall drop seen stating "FirewallL4" seen on Cisco IOS XE Catalyst SD-WAN Device
<a href="#">CSCwb32059</a>	Cellular interface tracker down but NAT route persists in the Service VPN Routing Table
<a href="#">CSCwc44851</a>	Bootstrap failing on c8300 on 17.9
<a href="#">CSCwc96444</a>	Cisco IOS XE Catalyst SD-WAN Device router is not programming correct next-hop for unicast prefix with multicast config present
<a href="#">CSCwc89328</a>	Multiple C8500s on Cisco SD-WAN experienced crashes every 4-5min
<a href="#">CSCwd06118</a>	IKEv2 Cert-based IPSEC not working between Cisco IOS-XE and AWS
<a href="#">CSCwc77183</a>	Packet duplication is causing drops in payment transactions with Cisco SD-WAN GenericDrop code.
<a href="#">CSCwc20170</a>	C8500 cEdgeCisco IOS XE Catalyst SD-WAN Device Reloads Unexpectedly due to Critical FTMD Fault when VRF Configuration is Pushed
<a href="#">CSCwd45894</a>	Cisco Catalyst SD-WAN ACL TCAM not in sync with configuration
<a href="#">CSCwc52538</a>	Cisco SD-WAN flows are not distributed and load-balanced evenly and consistently
<a href="#">CSCwc45950</a>	ZBFW self zone policy drops ssh session on Mgmt-intf 512 ports
<a href="#">CSCwb90252</a>	Automatically freeing up filesystems stale image or recovered folder (lost+found)
<a href="#">CSCwc79145</a>	Throughput degrades when local TLOC specified in Data Policy goes down
<a href="#">CSCwc32595</a>	BFD sessions remains down if interface flap form up/down/up
<a href="#">CSCwb48953</a>	Cisco IOS XE Catalyst SD-WAN Device speed test failing with "Device Error: Speed test in progress"

Identifier	Headline
<a href="#">CSCwd11365</a>	Needs cert update - Azure CGW creation fails due to NVA provisioning failure
<a href="#">CSCwc95218</a>	C8300 with 5G module P-5GS6-GL is losing cellular config at each boot after upgrading to 17.9.1
<a href="#">CSCwc28587</a>	C8300 : Crashed without generating any core (Critical process plogd fault on rp_0_0 (rc=75)
<a href="#">CSCwd13352</a>	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.
<a href="#">CSCwc77177</a>	BFD and control packets are dropped when ACL is applied on giga to which loopback is bind
<a href="#">CSCwc68132</a>	SIG tunnel tracker packets are dropped by firewall with self zone policy
<a href="#">CSCwb67406</a>	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
<a href="#">CSCwd45508</a>	Cisco IOS XE Catalyst SD-WAN Device does not form BFD across Serial link when upgrading from 17.3.3 to 17.6.x
<a href="#">CSCwd33966</a>	Unable to configure the local BGP as-path-list via Cisco SD-WAN Manager.
<a href="#">CSCwa14636</a>	Cisco IOS XE Catalyst SD-WAN Device stopped forwarding traffic. Suspect OMPD is busy
<a href="#">CSCwd15560</a>	With 2 sequences, should not skip if the match is different and action is same
<a href="#">CSCwd13050</a>	After upgrade to 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.
<a href="#">CSCwd12955</a>	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured
<a href="#">CSCwd37410</a>	0365 and MS Teams applications access issues when using DIA with app-list match in data-policy
<a href="#">CSCwd36621</a>	Cisco IOS XE Catalyst SD-WAN Device: CERM may kick in due to IPSec sessions initiated for on-demand tunnels
<a href="#">CSCwd44586</a>	Cisco SDWAN Cisco IOS XE Catalyst SD-WAN Device - Login banner config is changed after upgrade to 17.6.3a
<a href="#">CSCwd44006</a>	Control Connection on Cisco IOS XE Catalyst SD-WAN Device doesn't come-up with reverse proxy using Enterprise Certificate

Identifier	Headline
<a href="#">CSCwd29334</a>	Upgrade failures due to inability to establish netconf connection from Cisco SD-WAN Manager to upgrade-confirm
<a href="#">CSCwd34941</a>	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
<a href="#">CSCwb43423</a>	Cisco IOS XE Catalyst SD-WAN Device image installation fails
<a href="#">CSCwb16723</a>	Traceroute not working on Cisco IOS XE Catalyst SD-WAN Device with NAT
<a href="#">CSCwa67886</a>	UDP based DNS resolution doesn't work with IS-IS EMCP on Cisco IOS XE Catalyst SD-WAN Device
<a href="#">CSCwb33968</a>	Cisco Cisco SD-WAN Manager failed to display active flows when flow count is high on the device.
<a href="#">CSCvz84588</a>	Destination prefix packets getting dropped because forwarding plane is not programming the next hop.
<a href="#">CSCwb59736</a>	CSR BFD tunnel are zero with Cisco Catalyst SD-WAN version 17.03.03.0.7
<a href="#">CSCwb44275</a>	Simulated flows with PPPoE with NAT DIA result in crash consistently
<a href="#">CSCwa57873</a>	Incorrect reload reason - Last reload reason: LocalSoft for Netconf Initiated request
<a href="#">CSCwb51595</a>	Missing IOS config (voice translation rule) on upgrade from 17.3 to 17.6
<a href="#">CSCwb18315</a>	Umbrella DNS security policy doesn't work with Cloud onRamp with SIG tunnels
<a href="#">CSCwa49721</a>	Cisco Catalyst SD-WAN HUB with firewall configured incorrectly dropping return packets when routing between VRFs
<a href="#">CSCwb18223</a>	SNMP v2 community name encryption problem
<a href="#">CSCwb39098</a>	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
<a href="#">CSCwc32595</a>	bfd sessions remains down if interface flap form up/down/up
<a href="#">CSCwc20075</a>	Unable to switch the technology from 4g to 3g

Identifier	Headline
<a href="#">CSCwc38529</a>	[17.6] Traffic seems not inspected by UTD when umbrella is set
<a href="#">CSCwc55467</a>	BFD Tunnel on Cisco SDWAN router is not staying up, 1 out of 40 tunnels.
<a href="#">CSCwc20170</a>	C8500 Cisco IOS XE Catalyst SD-WAN Device reloads unexpectedly due to critical FTMD fault when VRF configuration is pushed
<a href="#">CSCwc37465</a>	Static NAT configuration in CLI with the no-alias keyword cannot be retrieved via NETCONF/YANG
<a href="#">CSCwc27208</a>	BFD sessions not coming UP because of ANTI-REPLAY-FAILURES
<a href="#">CSCwc06047</a>	Cisco Catalyst SD-WAN tunnel keeps on flapping on dialer interface with 17.3.6 throttle image for TSN platform
<a href="#">CSCwc63337</a>	Destination not reachable if configured as a next for a static route resolvable via non /32 OMP
<a href="#">CSCwc52538</a>	Cisco Catalyst SD-WAN flows are not distributed and load-balanced evenly and consistently
<a href="#">CSCwc23077</a>	Firewall drop seen stating "FirewallIL4" seen on Cisco IOS XE Catalyst SD-WAN Device
<a href="#">CSCwb74821</a>	Yang-management process confd is not running, controller mode 17.6.2a
<a href="#">CSCwb67406</a>	The IPSLA udp-jitter V3 (optimize timestamp+precision microseconds) does not work on C8500
<a href="#">CSCwc53885</a>	Cisco IOS XE Catalyst SD-WAN Device "no ip nat" config is allowed to be committed and removes nat routes among other nat config
<a href="#">CSCwc59650</a>	show sdwan app-fwd cflowd flows vpn X format tabled does not show all flows for vpn X
<a href="#">CSCwc44851</a>	Bootstrap failing on c8300 on 17.9
<a href="#">CSCwc55684</a>	Cisco Catalyst SD-WAN SIG GRE: Layer 7 Health check doesn't work on Loopback interfaces
<a href="#">CSCwc42978</a>	ISR1100-4G loses all BFD sessions with Invalid SPI
<a href="#">CSCwc54463</a>	Cisco IOS XE Catalyst SD-WAN Device C1121x-8P LAN Module is down when high CPU noticed
<a href="#">CSCwc55260</a>	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

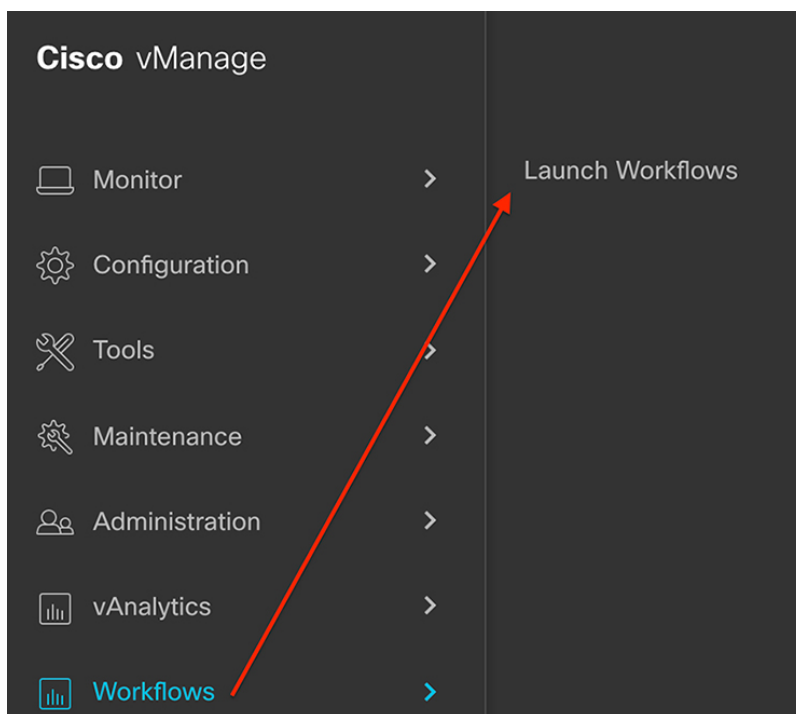
This section presents a comparative summary of the significant changes between Cisco vManage 20.8.x and Cisco vManage Release 20.9.1.

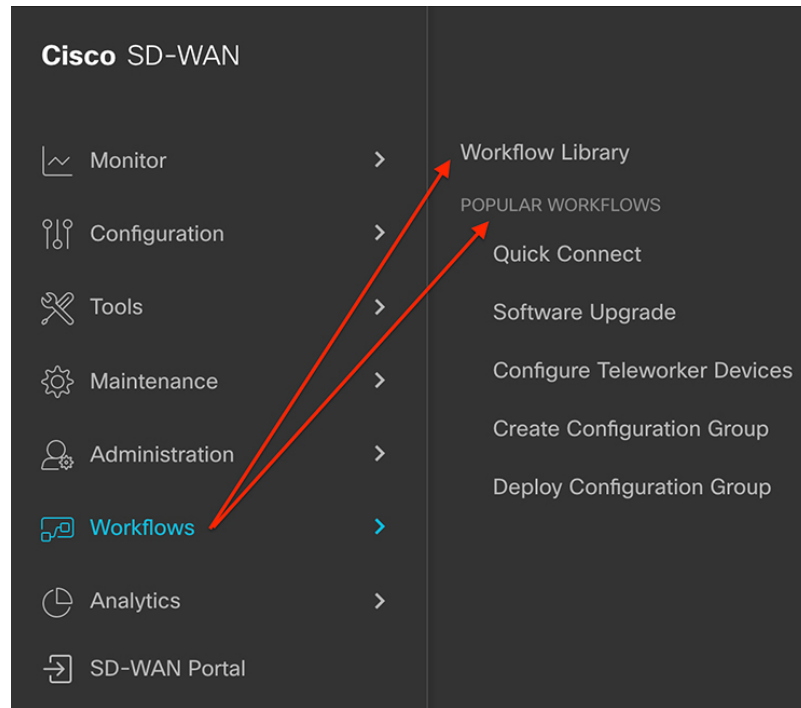
### Workflows Menu

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

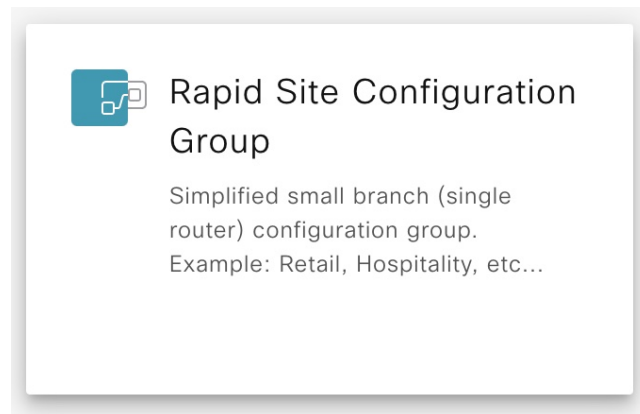
- The **Launch Workflows** submenu is renamed as **Workflow Library**.
- The **Popular Workflows** section is introduced for easy and quick access to the workflows.

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

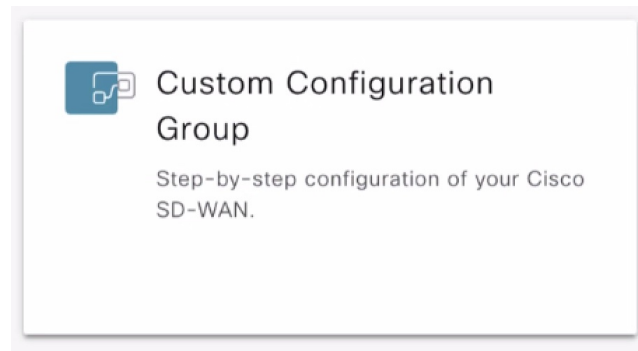


*Figure 2: Workflows Menu in Cisco SD-WAN Manager 20.9.1*

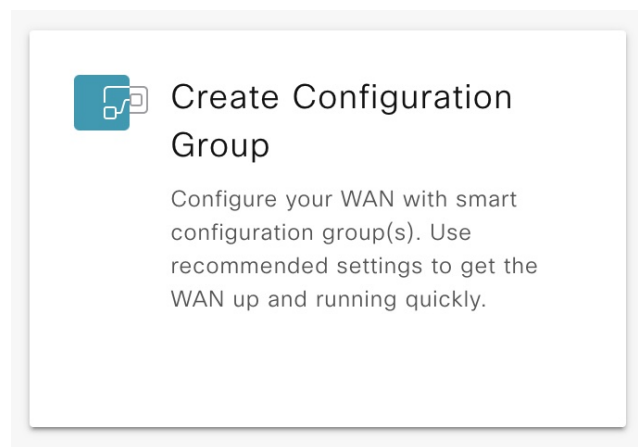
- The **Rapid Site Configuration Group** and **Custom Configuration Group** workflows are removed, and the **Create Configuration Group** workflow is introduced.

*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**

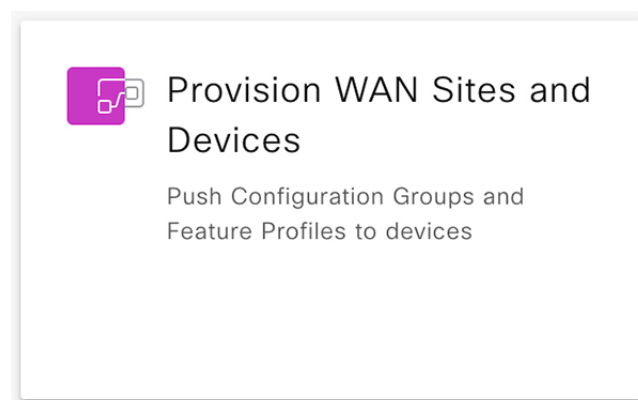


**Figure 5: Create Configuration Group Workflow in Cisco SD-WAN Manager 20.9.1**

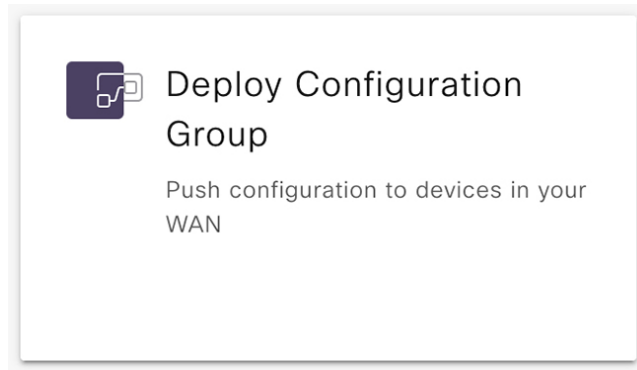


- The **Provision WAN Sites and Devices** workflow is renamed as **Deploy Configuration Group**.

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



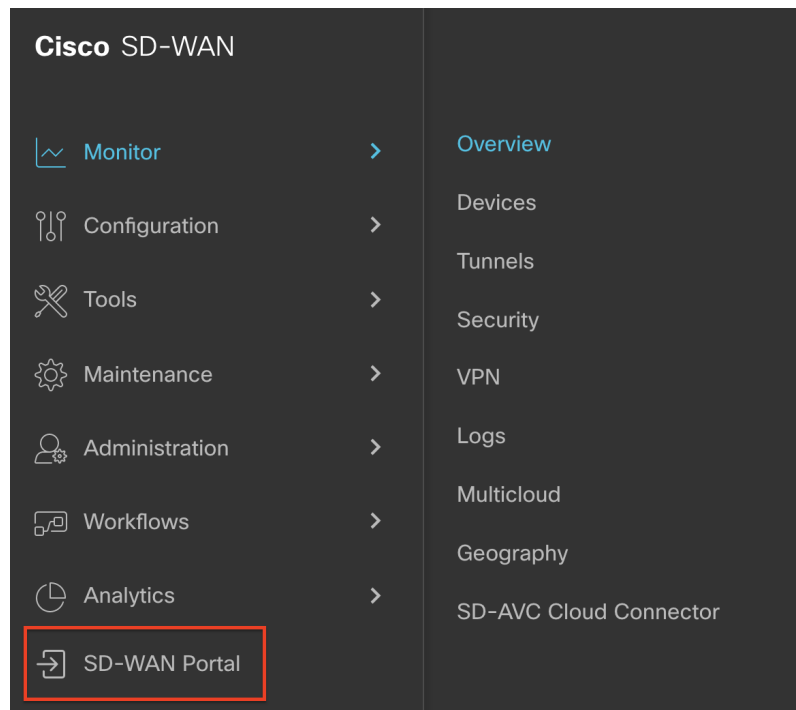
*Figure 7: Deploy Configuration Group Workflow in Cisco SD-WAN Manager 20.9.1*



### 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

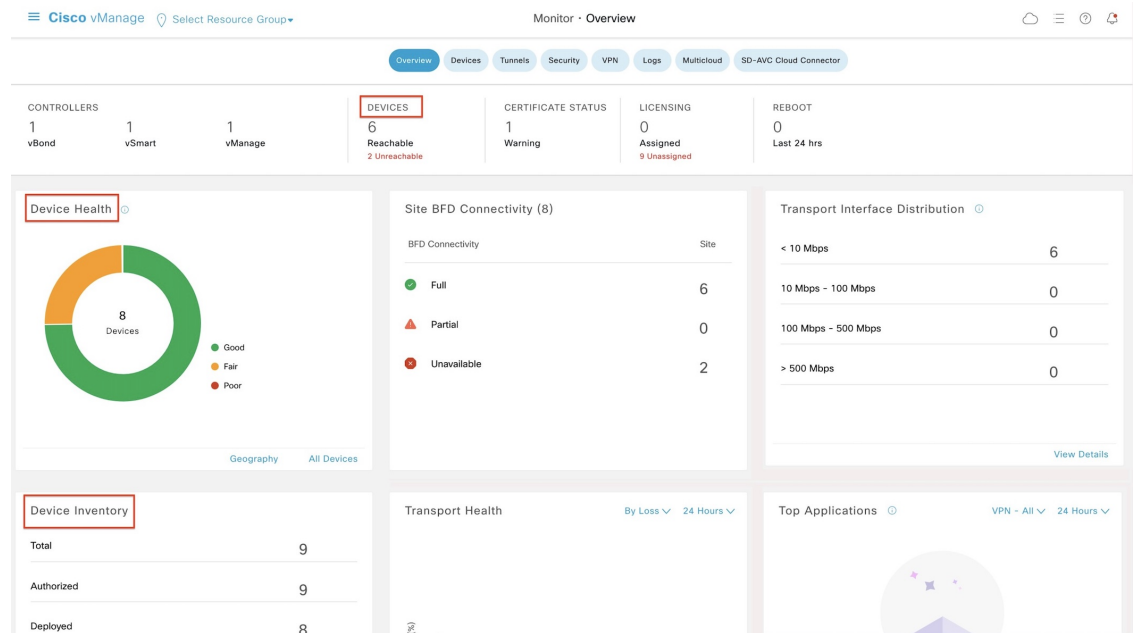
In Cisco vManage Release 20.9.1, the labels of the following UI elements have changed:

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

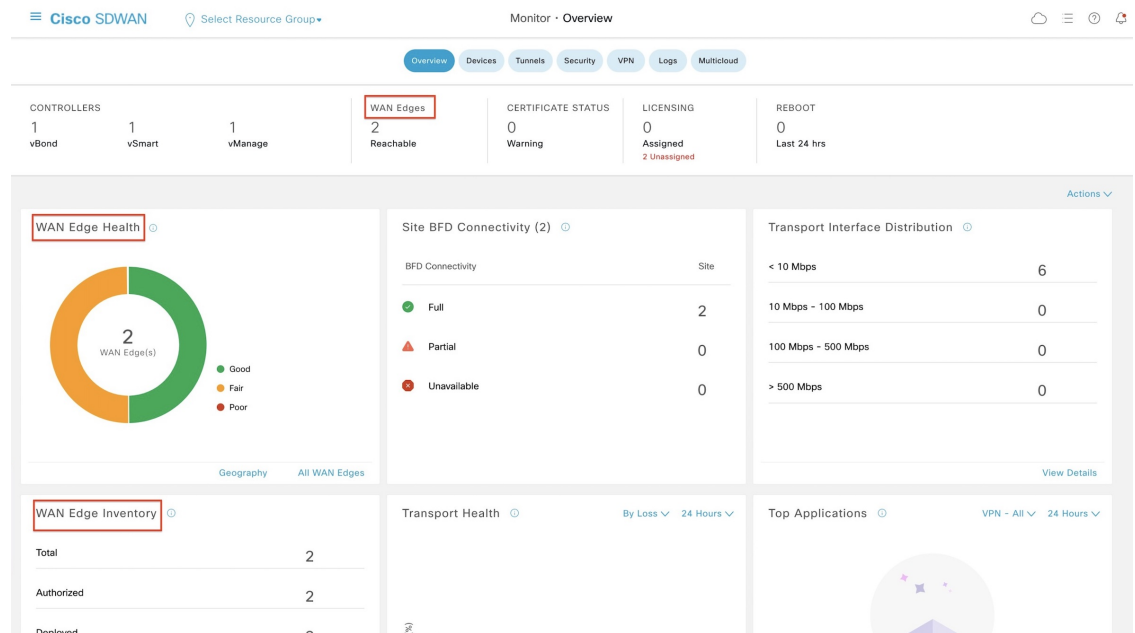


## • Device Inventory to WAN Edge Inventory

**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**



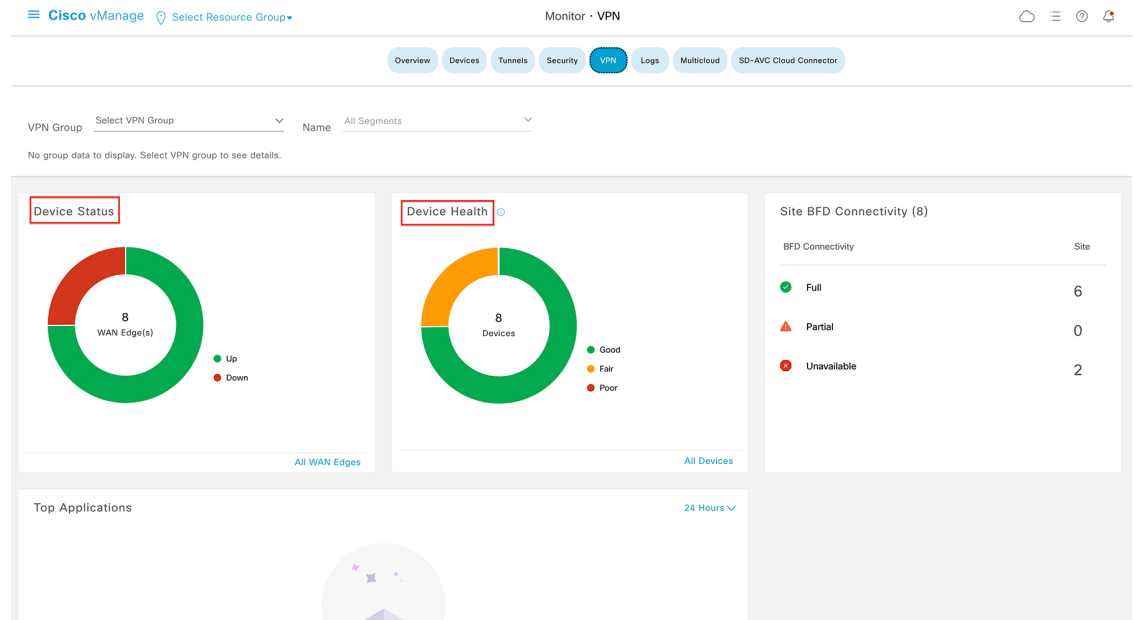
## Monitor VPN Page

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

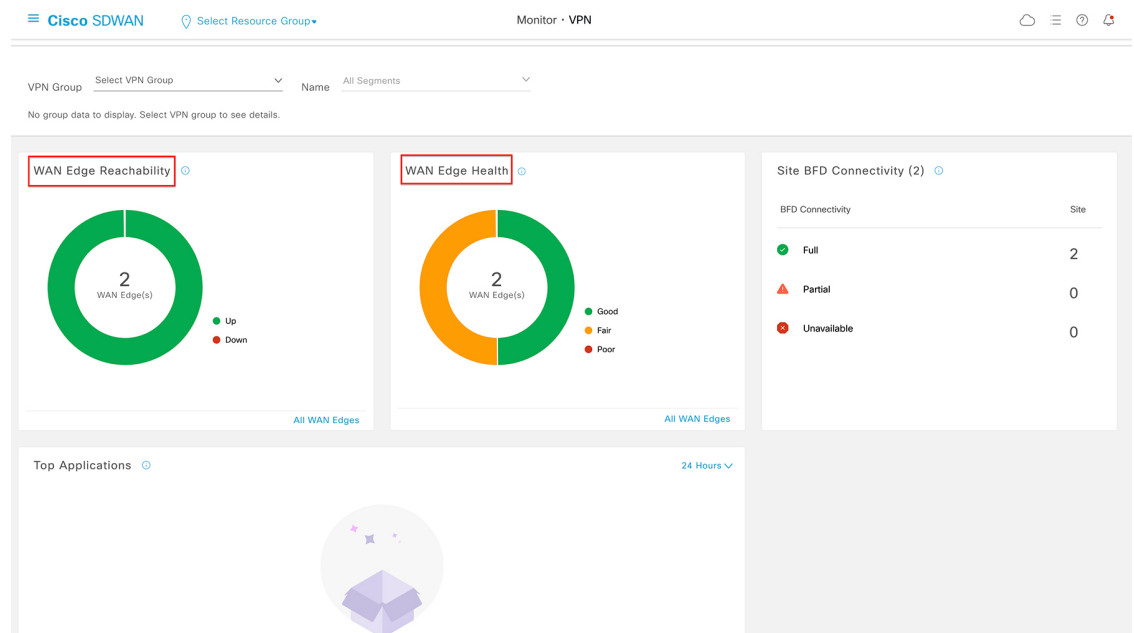
- Device Status to WAN Edge Reachability

## • Device Health to WAN Edge Health

**Figure 11: Monitor VPN Page in Cisco 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**

**Test** [Edit](#)

Created: Apr 28, 2022 by admin Last Updated: Apr 28, 2022 Device Family: cedge

**Feature Profiles** Associated Devices

**Feature Profiles - Unconfigured**

The feature profiles below have not been configured and will be required in order to deploy to your devices.

**CLI**  
CLI | v1.0

[Start Configuration](#)

**Feature Profiles - Configured**

The feature profiles below have been configured. Feel free to edit or remove them, as needed. Any edit or removal will not effect deploy devices they will just be marked out of sync.

**Test1**  
transport | v1.0

Add WAN Transport configuration

[Start Configuration](#)

**Test2**  
service | v1.0

Add LAN Segment configuration

[Start Configuration](#) [Start Configuration](#) [Start Configuration](#) [Start Configuration](#)

**Test**  
system | v1.0

Configures NTP Server and System wide settings like hostname, system IP, Site ID, Banner messages, BGD and OMP, IPSec Security

[aaa](#) [service](#) [omp](#) [banner](#) [logging](#) [bfd](#) [basic](#)

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

**config-new** [Edit](#)

Created: May 25, 2022 by admin Last Updated: May 25, 2022 Device solution: sdwan

**Feature Profiles** Associated Devices

**Feature Profiles - Configured**

The feature profiles below have been configured. Feel free to edit or remove them, as needed. Any edit or removal will not effect deploy devices they will just be marked out of sync.

**System Settings Profile - config-new\_Basic** Shared: 1 Groups

Search Table

[Add Feature](#)

Name	Description	Parcel Type	Actions
AAA	AAA Profile Description of config-new_Basic	aaa	...
BFD	BFD Description of config-new_Basic	bfd	...
Banner	Banner Description of config-new_Basic	banner	...
Basic	Basic Setting Description of config-new_Basic	basic	...
Global	Global Description of config-new_Basic	global	...
Logging	Logging Description of config-new_Basic	logging	...
NTP	NTP Description of config-new_Basic	ntp	...
OMP	OMP Description of config-new_Basic	omp	...

## 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

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

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

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

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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

---

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

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

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

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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

© 2022–2025 Cisco Systems, Inc. All rights reserved.