Release Notes for Cisco Catalyst SD-WAN Control Components Release 20.9.x

First Published: 2022-08-01

Last Modified: 2024-04-06

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 Catalyst SD-WAN Control Components Release 20.9.x

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

These release notes accompany the Cisco Catalyst SD-WAN Control Components, Release 20.9.x, which provides Cisco Catalyst SD-WAN capabilities. They include release-specific information for Cisco Catalyst SD-WAN Controllers, Cisco Catalyst SD-WAN Validators, Cisco SD-WAN Manager as applicable to Cisco Catalyst SD-WAN.

Related Releases

For release information about Cisco IOS XE Catalyst SD-WAN devices, refer to Release Notes for Cisco IOS XE Catalyst SD-WAN device, Cisco IOS XE Catalyst SD-WAN Release 17.9.x.

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

What's New for Cisco Catalyst SD-WAN Control Components Release 20.9.x

Cisco is constantly enhancing the Cisco Catalyst SD-WAN solution with every release and we try and keep the content in line with the latest enhancements. The following table lists new and modified features we documented in the Configuration, Command Reference, and Hardware Installation guides.

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.

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

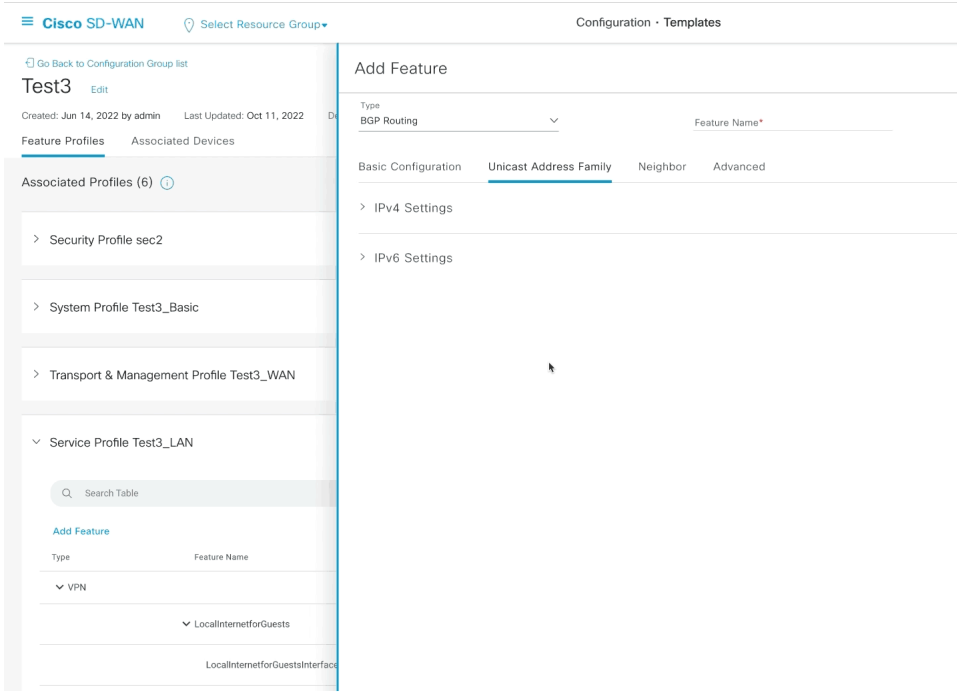
Feature	Description
Cisco Catalyst SD-WAN Analytics	

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

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

Feature	Description
Cisco Catalyst SD-WAN Systems and Interfaces	

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

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

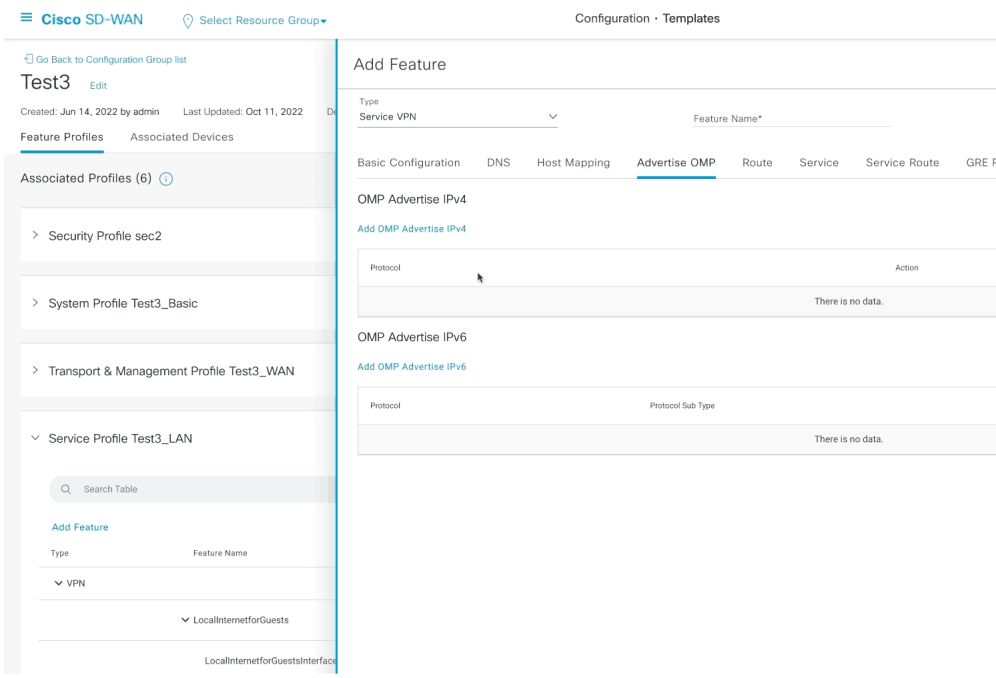
Feature	Description
	
Cisco Catalyst SD-WAN Monitor and Maintain	
Device Information	The **Monitor** > **Devices** page displays the devices that are newly added or synced to Cisco SD-WAN Manager using the options available on the **Configuration** > **Devices** page.
Cisco Catalyst SD-WAN Multi-Region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

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

Feature	Description
Cisco Catalyst SD-WAN Getting Started	

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

Feature	Description

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

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

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

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

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

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

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

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

What's New for Cisco SD-WAN Release 20.9.x

This section applies to Cisco vEdge devices.

Table 4: Cisco SD-WAN Release 20.9.2

Feature	Description
Systems and Interfaces	
Synchronized device lists in Cisco SD-WAN Manager	This feature synchronizes the device lists on the **Configuration** > **Devices** and **Monitor** > **Devices** pages. The **Monitor** > **Devices** page now displays the devices that are newly added or synced to Cisco SD-WAN Manager using the options available on the **Configuration** > **Devices** page.

Table 5: Cisco SD-WAN Release 20.9.1

Feature	Description
Cisco Catalyst SD-WAN Getting Started	
Support for License Management Using a Proxy Server	If you configure Cisco SD-WAN Manager to use a proxy server for internet access, Cisco SD-WAN Manager uses the proxy server to connect to Cisco SSM or an on-premises SSM.
Support for Managing Licenses Using Cisco Smart Software Manager On-Prem	Cisco SD-WAN Manager supports management of device licenses, using a Cisco SSM On-Prem license server. This is useful for organizations that use Cisco SSM On-Prem to accommodate a strict security policy that does not permit devices to communicate with Cisco SSM over a direct internet connection.
Renew Device CSR	This feature allows you to reset the RSA private and public keys, and generate a CSR that uses a new key pair. In earlier releases, the generation of CSR used the existing key pair.
Systems and Interfaces	
Hardened Passwords	This feature lets you configure Cisco SD-WAN Manager to enforce predefined medium-security or high-security password criteria.
Network Hierarchy and Resource Management	This feature enables you to create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. The network hierarchy and the associated resource IDs, including region IDs and site IDs, help you apply configuration settings to a device. In addition, the introduction of the resource manager in Cisco SD-WAN Manager automatically manages these resource IDs, thereby simplifying the overall user experience of Cisco SD-WAN. You can create a region only if you enable the **Multi-Region Fabric** option in Cisco SD-WAN Manager.
Co-Management: Improved Granular Configuration Task Permissions	To provide a user with the ability to self-manage specific configuration tasks, you can assign the user permissions to configure specific features while excluding others. This feature introduces numerous new permission options, enabling fine granularity in determining which configuration task permissions to provide to a user.

Feature	Description
RBAC for Security Operations and Network Operations Default User Groups	This feature provides the following default user groups: • network_operations user group for non-security policies • security_operations user group for security policies RBAC for policies allows you to create users and user groups with the required read and write permissions for security and non-security policies. Users can perform configuration and monitoring actions only for the authorized policy type.
Flexible Tenant Placement on Multitenant Cisco SD-WAN Controller	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.
Routing	
Route Leaking between Inter-Service VPN	This feature allows you to leak routes between service VPNs on the same edge device.
Policies	
Custom Applications	This feature enables you to define custom applications using Cisco Software-Defined Application Visibility and Control (SD-AVC) support. This feature is available only on Cisco vEdge devices.
Application-Aware Routing for Hub and Spoke	This feature allows you to configure AAR for traffic coming from tunnel to tunnel on Cisco Catalyst SD-WAN devices. Prior to Cisco SD-WAN Release 20.9.1, AAR policy is applied only for packets coming from service going to tunnel. With this feature, you can apply AAR policy for packets coming from tunnel to tunnel as per SLA requirements.
Lawful Intercept	This feature enhances the support for Lawful Intercept in Cisco Catalyst SD-WAN. Cisco Catalyst SD-WAN's Lawful Intercept feature enables Cisco SD-WAN Manager and Cisco SD-WAN Controller to provide the key information to LEA so they can decrypt the Cisco Catalyst SD-WAN IPsec traffic captured by the MSP.
Security	
Global SIG Credentials Template	With this feature, create a single global SIG Credentials template for each SIG provider (Cisco Umbrella or Zscaler). When you attach a SIG template to a device template, Cisco SD-WAN Manager automatically attaches the applicable global SIG Credentials template to the device template.
Disable Weak SSH Encryption Algorithms	This feature allows you to disable weaker SSH algorithms that may not comply with certain data security standards.
Cisco Catalyst SD-WAN Monitor and Maintain	

Feature	Description
Access TAC Cases from Cisco SD-WAN Manager	This feature allows you to access Support Case Manager (SCM) wizard using Cisco SD-WAN Manager. You can create, view, or edit the support cases directly from Cisco vManage without having to go to a different Case Manager portal.
Analyze the Health of the Cisco SD-WAN Manager Cluster and Cluster Services Using the CLI	With this feature, you can analyze the health of the Cisco SD-WAN Manager cluster and the status of the cluster services using the **request nms cluster diagnostics** CLI command.
Additional Real Time Monitoring Support for AppQoE and Other Configuration Options	This feature adds support for real-time monitoring for AppQoE and other device configuration details. Real-time monitoring in Cisco SD-WAN Manager is similar to using **show** commands in the CLI of a device.
Compare Template Configuration Changes Using Audit Logs	This feature introduces a **Config Diff** option for audit logs of device templates and feature templates. The **Config Diff** option shows configuration changes made to the template, comparing the current configuration and previous configuration. The **Config Diff** option is available for audit logs to view the configuration changes when a template is not attached to a device.
Customizable Monitor Overview Dashboard in Cisco vManage	This feature adds customizability to the **Monitor Overview** dashboard. It gives you the flexibility to specify which dashlets to view and sort them based on your personal preferences.
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.
High Availability	
Configure Disaster Recovery Alerts	This feature provides support for configuring Cisco SD-WAN Manager alerts to generate an alarm and a syslog message for any disaster recovery workflow failure or event that occurs.

What's New for Cisco Catalyst SD-WAN Control Components Release 20.9.x

This section applies to Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator.

Table 6: Cisco vManage Release 20.9.3

Feature	Description
Inactivity lockout	This feature lets you configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.
Unsuccessful Login Attempts Lockout	This feature lets you configure Cisco SD-WAN Manager to lock out uses who made a designated number of consecutive unsuccessful login attempts within a designated period.
Duo Multifactor Authentication Support	This feature lets you configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to Cisco SD-WAN Manager.
Custom Domain Settings	This feaure lets you specify a domain other than the default cisco.com domain when you create a Cisco Catalyst SD-WAN cloud-hosted overlay.
Create Predefined Inbound Rules	This feature lets you specify trusted IP addresses that are applied automatically to any overlay that you create in the future, and optionally to existing overlays, under the Smart Account for which you configure this feature.

Software and Hardware Behavior Changes in Cisco Catalyst SD-WAN Control Components Release 20.9.5

Behavior Change	Description
You can deploy a Cisco Catalyst 8000v Edge Software instance as the Interconnect Gateway in the Equinix fabric.	The device support for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix is described in Restrictions for Cisco Catalyst SD-WAN Cloud Interconnect with Equinix.

Important Notes, Known Behaviors, and Workarounds

- If your ConfigDB (Neo4j) username contains a – (hyphen), the ConfigDB upgrade fails. For example, db-admin. Remove the hyphen before you upgrade the ConfigDB.
- From Cisco SD-WAN Release 20.4.1.1, Microsoft Azure environment is supported for deploying Cisco Catalyst SD-WAN Control Components (Cisco Catalyst SD-WAN Validator, Cisco SD-WAN Controller, and Cisco SD-WAN Manager). The support is limited to Cisco Catalyst SD-WAN cloud-based deployments only.
- If SD-AVC is enabled using Cloud Connector or custom applications while upgrading from Cisco vManage Release 20.3.1 to Cisco vManage Release 20.6.1 and later releases, during the upgrade, a defect CSCwd35357 is impacting the data plane. We strongly recommend you to contact the Cisco TAC to perform a workaround while upgrading.

- The bugs CSCwd78294 and CSCwd63915 are affecting user experience when Cisco SD-WAN Manager is running Cisco vManage Release 20.9.2. We recommend you upgrade to Cisco vManage Release 20.9.2.1 that has the latest build and provides you a seamless user experience. For more information see, the deferral notice.
- The bugs CSCwh16410, CSCwh48782, CSCwi45443 are affecting user experience when Cisco SD-WAN Manager is running Cisco Catalyst SD-WAN Control Components Release 20.9.5. We recommend you upgrade to Cisco Catalyst SD-WAN Control Components Release 20.9.5.1 that has the latest build and provides you a seamless user experience. For more information see, the deferral notice.

Cisco SD-WAN Manager Upgrade Paths

For information about Cisco SD-WAN Manager upgrade procedure, see Upgrade Cisco SD-WAN Manager Cluster.

Starting Cisco SD-WAN Manager Version	Destination Version								
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x	20.9.x
18.x/19.2.x	Direct Upgrade	Direct Upgrade		Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x

Starting Cisco SD-WAN Manager Version	Destination Version								
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x	20.9.x
			Check disk space* • If the disk space is more than 2GB: Direct Upgrade • If the disk space is less than 2GB: Step upgrade through 20.1 • If you are upgrading to 20.3.5, the available disk space should be at least 2.5 GB. For cluster						

Starting Cisco SD-WAN Manager Version	Destination Version								
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x	20.9.x
			upgrade procedure**: **request nms configuration-db upgrade** **Note**	We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.					

Starting Cisco SD-WAN Manager Version	Destination Version								
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x	20.9.x
20.1.x	Not Supported	Not Supported	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x	Step upgrade through 20.3.x

Starting Cisco SD-WAN Manager Version	Destination Version								
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x	20.9.x
20.3.x	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend that the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend that the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend that the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend that the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend that the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

Starting Cisco SD-WAN Manager Version	Destination Version								
	19.2.x	20.1.x	20.3.x	20.4.x	20.5.x	20.6.x	20.7.x	20.8.x	20.9.x
20.4.x	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.	Direct Upgrade For cluster upgrade procedure**: **request nms configuration-db upgrade** **Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.
20.5.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade	Direct Upgrade
20.6.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade
20.7.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade
20.8.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade

*To check the free disk space using CLI,

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

**Cluster upgrade must be performed using CLI

- Use the following command to upgrade the configuration database. This must be done on only one node in the cluster:

```
request nms configuration-db upgrade
```

Note We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later.

- Enter login credentials, if prompted. Login credentials are prompted if all Cisco SD-WAN Manager server establish control connection with each other. After a successful upgrade, all configuration-db services are UP across the cluster and the application-server is started.Enter login credentials, if prompted. Login credentials are prompted if all Cisco SD-WAN Manager server establish control connection with each other. After a successful upgrade, all configuration-db services are UP across the cluster and the application-server is started.

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 Catalyst SD-WAN Control Components Release 20.9.5.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.5.1

Bug DI	Description
CSCwi45443	The vdaemon file is incomplete when generating a Cisco SD-WAN Manager admin-tech using GUI
CSCwh16410	Admin tech generation for Cisco SD-WAN Manager is failing in UI
CSCwh48782	TACACS netadmin users not able to acess vshell on 20.12

Bugs For Cisco Catalyst SD-WAN Control Components Release 20.9.5

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.5

Identifier	Headline
CSCwd95581	VRRP timer in Cisco SD-WAN Manager UI - default 100ms
CSCwf68955	Cisco SD-WAN Manager Log Poisoning bypass

Identifier	Headline
CSCwf68959	Cisco SD-WAN Manager Audit Log CSV payload injection
CSCwf75967	Cisco SD-WAN Manager Malicious File Upload vulnerability
CSCwc51421	Cisco SD-WAN Control Components 20.10 : nested feature profile RBAC is not handled properly.
CSCwh25000	Cannot overwrite a FW security policy with a CLI add-on template.
CSCwc08313	System does not throw an error message for the overlapping policies in some cases.
CSCwi27589	Cloud on ramp for multicloud deploy fails with error : Azure Error: Request Disallowed By Policy
CSCwi04802	Create CGW failing with "Public access is not permitted on this storage account".
CSCwe34379	The Cisco SD-WAN Manager access failed when accessingCisco SD-WAN Manager using DNS record
CSCwd94839	Cisco SD-WAN Manager GUI becomes unavailable due to authentication errors against configuration-db.
CSCwd16027	Unable to generate report from Cisco SD-WAN Manager for SLP Offline mode - Error occurred while generating report.
CSCwf75554	3 node 20.6 cluster reporting error for 1 node:Unable to authenticate for for device IP Nio2Session
CSCwd73212	The ciscotacro and ciscotacrw login on Cisco SD-WAN Manager is not creating an entry in audit log.
CSCwe14017	The 20.6.5 Cisco SD-WAN Validator and Cisco SD-WAN Controller upgrade fail via Cisco SD-WAN Manager UI
CSCwh02439	Cisco SD-WAN Manager- Unable to add devices to Cloud on Ramp for SaaS due to timeout while loading device list.
CSCwe80348	Cluster creation may fail due to store ID mismatch in neo4j.
CSCwe26011	Cisco SD-WAN Manager is not generating alarm notifications to be sent to Webhooks server.
CSCwf81695	Unable to add more than 30 VPN Interface SVI.
CSCwe32116	Cisco SD-WAN Manager : DSPFarm template error "Duplicate value:mediaresourcegroupname"
CSCwc44186	Getting maximum session limit reached when trying to ssh to edge devices from Cisco SD-WAN Manager.
CSCwi03952	Cisco SD-WAN Manager template push failure | Failed to update configuration - CLI generation failed.

Identifier	Headline
CSCwh04968	Control Session PPS increase and reset during the upgrade for Cisco vEdge Device.
CSCwe07709	The Cisco SD-WAN Controller reboots with kernel panic, customer netwrok outage because of OMP State becomes Rej,Inv,U.
CSCwf48674	The Cisco IOS XE Catalyst SD-WAN device unified security policy template fails to enable geo database.
CSCwf98777	The Cisco SD-WAN Controller policy is not sending the updated TLOC information.
CSCwh22127	Software initiated reboot due to OMPD crash (segmentation fault).
CSCwh01870	Template push failed post Cisco SD-WAN Manager upgrade from 20.4 to 20.9 "udp udp-src-dst-port-list source range".
CSCwc05127	Breakdown of U-Plane communication after updating Cisco SD-WAN Controller CiscoPKI certificate.
CSCwf07155	"Set CSR Properties" for Controllers Cert Auth setting on Cisco SD-WAN Manager GUI is not getting disabled.
CSCwe57259	Template pushed with wrong APN settings. The Cisco SD-WAN Manager shows wrong APN config even after rollbacked.
CSCwh45608	20.9: IP Subnet Pool is not discovered when creating Azure CGW using existing vHUB.
CSCwb43140	java.lang.OutOfMemoryError: unable to create native thread (may lead to sysmgr got signal 11 crash)
CSCwi59963	DCA process continuously restarting after upgrade to 20.9.3.2.
CSCwf53131	Login via Radius is working but Usergroup is basic instead of netadmin.
CSCwh73298	After upgrading the Cisco SD-WAN Manager from 20.6.x to 20.9.3 ES, the standby Cisco SD-WAN Manager reports down status.
CSCwf38317	Syntax error when changing rule action from "drop log" to "inspect" for ZBFW template
CSCvz70097	Cisco SD-WAN Manager DSPFarm CUCM Template Dialog UI issues.
CSCwh18874	Replication takes 4+ hours to inject the 100MB of data on standby cluster-No Make Primary to switch
CSCwh46024	Cisco SD-WAN Manager is not starting new traces due to high scaled full mesh network.
CSCwh84962	The Cisco SD-WAN Controller withdraws TLOC RIB out after going into GR
CSCwh26907	Cisco SD-WAN Manager GUI SaaS Probe Endpoint Type URL is not allowing to use "-" character as value.
CSCwf40110	The option to add Switchport in the Configuration Group Templates is not available.
CSCwe31884	RBAC Configurational Group bug on 20.9.1 Software Version

Identifier	Headline
CSCwf95317	Devices are not receiving the preference via the policy in a Multi-Tenant environment.
CSCwh83203	MT: Centralized policy push with overlapping sites is returing success but Cisco SD-WAN Controller rejects it.
CSCwh24243	Suppress OMP Advertisement of Stale versioned TLOCs on Cisco SD-WAN Controller.
CSCwd53871	Filtering doesnot work for real-time OMP commands on Cisco SD-WAN Manager 20.6.
CSCwc47669	Cisco SD-WAN Manager cannot edit ZBFW policy.
CSCwh12619	"Routing DNA Essentials: Tier 0: 05M" is not available to choose in Cisco SD-WAN Manager GUI
CSCwh93441	[Cisco SD-WAN Manager] Unable to login SSH including ciscotacro/ciscotacrw
CSCwi21156	SDCI-Azure connection creation failsAzure Error:PublicIpWithBasicSkuNotAllowedOnExpressRouteGateways
CSCwh66310	Intermittently the SSO user with tenantadmin privilege only getting basic access.
CSCwh55434	In 3 memeber Elastic cluster , 1 FOLLOWER exibiting 96% CPU Utilization due to WRITE Threads
CSCwi30235	Issue with accessing Cisco SD-WAN Manager 20.6.6 GUI using upper-case letter on TACACS username
CSCwe90415	Massive update for Feature Template fails.
CSCwi05515	DR replication taking 2 hours for ~100 MB Size
CSCwh24335	Manipulate driver of Neo4j and ES to use static logger instead of new logger (Cisco SD-WAN Manager Slowness 20.6)
CSCvt47226	Routes missing on a SD-WAN Edge router in a graceful-restart scenario.
CSCwe87281	Requirement to support recommended DH groups from Umbrella for IKEv2 (SIG Template).
CSCwf49674	Cisco SD-WAN Manager is modifying load_balance .json leading to the edges to be disconnected.
CSCwh18738	Licenses unapplied from License Management in Cisco SD-WAN Manager after DR failover/failback.
CSCwi72014	CDCS Tenant - SSH tool not working
CSCwh22202	Overlay not coming up for Cisco hosted controllers - Post call getting mapped with wrong datastore.

Open Bugs for Cisco SD-WAN Controllers Release 20.9.5

Identifier	Headline
CSCwi43016	Need pop-up to display warning banner on 20.9 and 20.12 stating "SHA/AES-128 deprecation"
CSCwi45443	The vdaemon file is incomplete when generating a Cisco SD-WAN Manager admin-tech using GUI
CSCwh16410	Admin tech generation for Cisco SD-WAN Manager is failing in UI
CSCwh48782	TACACS netadmin users not able to acess vshell on 20.12
CSCwf34015	Unable to push template due to "no ip cef distributed"
CSCwi43409	Cisco SD-WAN ManagerCisco SD-WAN Manager 20.9/20.12: enforce character length validation for user, usergroup, password via confD
CSCwh97427	RADIUS user with username format domain\xxxx get's logged out without minutes of logging in.
CSCwi62044	HTTP 401 response when creating custom applications on Cisco SD-WAN Manager after upgrade.
CSCwi59683	MT Controllers - show control connection history doesn't list org name
CSCwi27360	The customer is seeing Unable to attach templates for some Cisco IOS XE Catalyst SD-WAN devicev- C1121x, on 20.9.4.1/ 17.9.4a

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.4.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.4.1

Identifier	Headline
CSCwh22202	Overlay not coming up for Cisco hosted controllers - Post call getting mapped with wrong datastore

Bugs For Cisco Catalyst SD-WAN Control Components Release 20.9.4

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.4

Identifier	Headline
CSCwc51421	20.10 : nested feature profile RBAC is not handled properly
CSCwd73212	The ciscotacro and ciscotacrw login on Cisco SD-WAN Manager is not creating an entry in audit log
CSCwd94301	MTT correlation engine not generating OMP Alarms from OMP Event received from Cisco SD-WAN Controller.

Identifier	Headline
CSCwb91924	Cisco SD-WAN Manager 20.8.1 "Error in generating configuration diff for the device" template with SIP commands
CSCwe54012	Neo4j not updating the ControlWanInterface info when Operational status changes
CSCwf21372	Cisco SD-WAN Manager does not recognize the resource group for resource group admin login via TACACS
CSCwc65025	The email notifications failing when Security is set as TLS with Gmail SMTP
CSCwd60889	The CPU average values reported to Cisco SD-WAN Manager are incorrect
CSCwf53131	Login via Radius is working but Usergroup is basic instead of netadmin
CSCwe30924	The removal of OU field in Cisco SD-WAN Manager for CSR of web-server certificate
CSCvz70097	Cisco SD-WAN Manager DSPFarm CUCM Template Dialog UI issues
CSCwf50089	Template push fails when ZBFW policy has sequences matching UDP ports 500/4500 in Cisco SD-WAN Manager 20.9
CSCwf03555	Cisco SD-WAN Manager is unable to parse certain timezones and is triggering certificate installation process
CSCwe34081	in Cisco SD-WAN Manager db, HSEC license node is showing duplicate Device IPs for UUIDs
CSCwe49214	Backend changes to allow all the characters that are allowed by CSSM
CSCwe12396	Max netconf sessions reached in confd which causes login failure for Cisco SD-WAN Manager
CSCwd54278	The aaamgr process restarts unexpectedly
CSCwe45436	/dataservice/device/cellular/hardware?deviceId return 400 in 20.6 Cisco SD-WAN Manager for Nutella deviecs
CSCwf09036	Cisco SD-WAN Manager configures incorrect IKEv2 lifetime for IPsec tunnels
CSCwd37096	Enabled usage but prepaid consumption - Product instance "UDI_PID:Cisco_Cisco SD-WAN Manager
CSCwf28362	Cisco SD-WAN Manager is not generating alarm notifications to be sent to Webhooks server.
CSCwd85558	The app-server java process is not initiating in 6 node 20.6 cluster
CSCwh03202	Cisco Catalyst SD-WAN Manager Unauthorized Access Vulnerability

Open Bugs for Cisco SD-WAN Controllers Release 20.9.4

Identifier	Headline
CSCwe60017	Cisco SD-WAN Manager CLI add-on template not pushing configuration on 20.9.x
CSCwf34015	Unable to push template due to "ip cef distributed"
CSCwf40110	The option to add Switchport in the Configuration Group Templates is not available

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.3.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.3.2

Identifier	Headline
CSCwf76218	Cisco SD-WAN Manager Unauthenticated REST API Access Vulnerability.
CSCwf82344	Cisco SD-WAN Manager Unauthenticated REST API Access Vulnerability.
CSCwf68936	Cisco SD-WAN vManage Authorization Bypass Vulnerability
CSCwf55823	Cisco Catalyst SD-WAN Manager Authorization Bypass Vulnerability

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.3.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.3.1

Identifier	Headline
CSCwf28118	Cisco vEdge: Certificate issue on Cisco vEdge devices

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.3

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.3

Identifier	Headline
CSCwc51421	20.10 : nested feature profile RBAC is not handled properly
CSCwd90919	Controller server logging priority config does not take effect
CSCwd79186	Cisco SD-WAN Manager generating corrupted TAR file for config-db backup on 20.3.4.0.5
CSCwd55169	Inactive user (disabled state) is able to login via CLI
CSCwd78294	Screen goes into loading when logged in as a basic user
CSCvz70097	Cisco SD-WAN Manager DSPFarm CUCM Template Dialog UI issues
CSCwb58176	SSO/ciscotacro/rw User Session invalidated when browser switches between Cisco SD-WAN Manager nodes in cluster

Identifier	Headline
CSCwe31950	Cisco SD-WAN Manager HTTP/HTTPS Settings break DR process even after adding the Cluster IPs in the non-proxy list
CSCwc87356	Cisco SD-WAN Manager "Renew Device CSR" task cannot be opened under completed tasks
CSCwd35596	Disaster Recovery warning shown when pushing templates to WAN Edge Devices
CSCwd37119	No Real Time Data or CPU/Memory data from ESR-6300-NCP-K9 17.9.1
CSCwe06555	Attaching license to device fails with Invalid saName error due special characters
CSCwd73212	ciscotacro and ciscotacrw login on Cisco SD-WAN Manager is not creating an entry in audit log
CSCwd90841	Cisco SD-WAN Manager: Dashboard: WAN Edge Health Widget shows invalid / unconfigured edges in poor health status
CSCwd46383	Cisco SD-WAN Software Denial of Service Vulnerability

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.3

Identifier	Headline
CSCwe27800	Cisco SD-WAN Manager IdP gives Invalid User or Password
CSCwe19378	Cannot sync HSEC using "Sync and Install HSEC Licenses" workflow if account pass phrase contain "#"
CSCwc66840	17.9 Config Preview for very large sec policy is taking too long compared to previous releases
CSCwe34379	Cisco SD-WAN Manager access failed when accessing Cisco SD-WAN Manager using DNS record
CSCwe34081	in Cisco SD-WAN Manager db, HSEC license node is showing duplicate Device IPs for UUIDs
CSCwe27472	Unable to install HSEC licenses from Cisco SD-WAN Manager to Cisco Catalyst 8000v
CSCwe25625	20.9.3: GCP: Service Discovery Failure while upgrading from 20.6.5 to 20.9.3
CSCwe31884	RBAC Configurational Group bug on 20.9.1 Software Version
CSCwd90586	Cisco SD-WAN Manager scrollbar is executing several API calls that slow down the performance
CSCwe26568	Cisco SD-WAN Manager multitenancy do not report licenses after provider credentials are changed.
CSCwd85558	"app-server" java process is not initiating in 6 node 20.6 cluster

Identifier	Headline
CSCwe30225	Cisco SD-WAN Manager 20.9.3: enabling inactivity days in 1 node of cluster is not reflecting on other nodes

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.2.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.2.1

Identifier	Headline
CSCwd78294	The screen keeps on loading when logged in as a basic user
CSCwd63915	Delay of around 6 hours to update "vmanage_auth_creds" after DR switchover

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.2

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.9.2

Identifier	Headline
CSCwc51421	Cisco Catalyst SD-WAN Control Components Release 20.10 : nested feature profile RBAC is not handled properly
CSCwd21136	UX2.0:20.9: VPN0-MGMT-VPN parcel IPv4 Static Route GW set to "Default" deploy failed
CSCwc13452	Memory leak in Cisco SD-WAN Controller -OMP
CSCwc43513	Stats are not getting processed on Cisco SD-WAN Manager GUI running 20.8.1 code
CSCwc60902	MTT unreachable device not showing up in common inventory page
CSCwc55684	Cisco Catalyst SD-WAN SIG GRE: Layer 7 health check doesn't work on loopback interfaces
CSCwb68441	VPN drop menu shows empty in NWPI when we intiate trace for first time
CSCwc50308	Frequent GC causing Server unavailable returing 503, GUI unaccessible intermittently
CSCwc71437	Controller group is not updated correctly when pushed from Cisco SD-WAN Manager
CSCwc72609	Incorrect behavior for ICMP redirect disable from WAN/LAN interface parcel
CSCwd21774	Saving WAN/LAN BGP parcel fails when BGP IPv4/IPv6 neighbor remoteAS is set to global integer value
CSCwc73492	Cisco SD-WAN Controllers release 20.10, Cisco vBond Hostname "NULL"
CSCwc70086	The side by side CLI compare does not put empty lines to see impact of change between 2 devices

Identifier	Headline
CSCwc75127	Cisco SD-WAN Manager Cisco IOS XE Catalyst SD-WAN Device BGP summary Counts are incorrect
CSCwb92586	Cisco SD-WAN Controllers Release 20.3.4, DR registration failed
CSCwc24241	Navigation to cancel from template "Confirm Load Method" popup does not cancel the operation
CSCvz70097	Cisco SD-WAN Manager DSPFarm CUCM template dialog UI issues
CSCwc41119	Duplicate role descriptors found in IDP metadata
CSCwa68925	Cisco SD-WAN Controllers Release 20.3.4 -- 2 minutes delay in Webhook event.
CSCwc51414	Hide the options from workflow side menu for the config group which are hidden in workflow page
CSCwd11782	UX2.0:20.9: LAN VPN10-99-Intf v4/v6 sec addr device specific variable giving dup'd names
CSCwc08514	Cisco SD-WAN Manager GUI and CLI has different syntax for usergroup
CSCwd04623	Packet Capture: VPN 65530 is not letting the loopback 65530 to be chosen
CSCwb95806	botocore.errorfactory.RegionDisabledException when doing VPC discovery with some regions inactive
CSCwc55697	Exception handling in Cisco SD-WAN Manager code does not return details about the exception we are hitting
CSCwb91858	Some template integer fields can be changed using the scroll wheel
CSCwc95935	DCA.py to remove the check for vanalytics to push telemetry data
CSCwa79824	Cisco SD-WAN Manager alarms logs are not cleared upon clicking "Mark All as viewed" when notification is 999+
CSCwc65037	MRF: OMPD crash in access Cisco vSmart while running policy cases in regression
CSCwc80099	After configdb credentials change, app-server is not coming up due to use of hyphen in credentials
CSCwc95869	Memory leak observed when adding a new node to a cluster

Open Bugs for Cisco SD-WAN Controllers Release 20.9.2

Identifier	Headline
CSCwd26472	Cisco SD-WAN Manager : DSPFarm template not accepting multiple variable fields for "CUCM Media Resource Name"
CSCwd36189	After upgrading to Cisco SD-WAN Manager 20.9.1-li template push and onboarding is no longer working

Identifier	Headline
CSCwd18028	After deleting CSP, New CCM bringup on existing CSP is stuck in "Initializing CCM" on MT cluster
CSCwc94093	Users are unable to login to Cisco SD-WAN Manager GUI
CSCwc66840	17.9 config preview for very large sec policy is taking too long compared to previous releases

Bugs for Cisco Catalyst SD-WAN Control Components Releases 20.9.1

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

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Releases 20.9.1

Identifier	Headline
CSCwb20070	20.8 : Disaster Recovery workflow fails during switchover
CSCwa39457	"Enforce Software Version (ZTP)" does not support version format for NFVIS-SDWAN-BRANCH
CSCvy19698	"Invalid user or password" errors on /dataservice/client/token when make multiple consecutive calls
CSCwb47038	UX2.0- SD-WAN Manager search option in WAN Tunnel not showing any result for tunnel endpoints
CSCvu76345	Class-map mapping issue for forward-class with QoS map and centralized policy
CSCwa76773	MT-tenant deletion causes VmonitorAgent log to get stuck and DCA doesn't send information to DCS
CSCwb38813	Secondary Cisco SD-WAN Manager continuously generates 'Data Center Down' alarms
CSCvz99938	OIB DayN: "Manage Network Design" button is disabled when add service. Need wait for task completed
CSCwb38187	Cisco SD-WAN Manager - 20.6.2.1 template push failed due to optional field - Invalid value for prefix
CSCwb37362	Unable to associate device to CG using tagging , seeing error CG already has a rule assigned
CSCwa54969	Cisco SD-WAN Manager iptables-dropped Log stopped after upgrading 20.6.1
CSCwb38655	Delete CSP(with CCM) followed by Add CSP - MT Cluster failed - Infra Exception
CSCwb04545	Not able to change config-db credentials on 20.6.2
CSCwb46339	UX2.0: Modify LAN Segment VPN number, the associated VPN interface name is not updated in workflow

Identifier	Headline
CSCwb48626	Quick Connect workflow still missing config group when tag is copied to a device
CSCwa85537	Cisco SD-WAN Manager UI stuck forever with {{msg1}} showed on UI while attaching Cisco IOS XE Device to device template failed
CSCvz62234	Cisco Catalyst SD-WAN Manager Unauthorized Configuration Rollback Vulnerability

Open Bugs for Cisco Catalyst SD-WAN Control Components Releases 20.9.1

Identifier	Headline
CSCwc04446	Default route is not installed in the routing table of VPN 0 if the VNIC is changed in OpenStack
CSCwc51421	20.9 : Teleworker feature profile RBAC is not handled properly
CSCwc80099	After configdb credentials change, app-server is not coming up due to use of hyphen in credentials
CSCwc43513	Stats are not getting processed on Cisco SD-WAN Manager GUI running 20.8.1 code
CSCwc51414	Hide the options from workflow side menu for the config group which are hidden in workflow page
CSCwc33733	Unable to activate/delete the software from Cisco SD-WAN Manager GUI
CSCwb52667	Multiple selection fr dropdown list to maintain the order in AAA Server Auth order field
CSCwc59865	Cisco SD-WAN Manager statistics-db heap-dump and thread-print commands are not supported
CSCwc61498	vnf-ha-net reused causing HA formation to FAIL
CSCwc05127	Breakdown of U-Plane communication after updating vSmart's CiscoPKI certificate
CSCwc37072	Template failed issue
CSCwc61220	Long processing time of replication keeping primary in mportPending and secondary in exportPending
CSCwc55697	Exception handling in Cisco SD-WAN Manager code does not return details about the exception we are hitting

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.

Related Documentation

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

Full Cisco Trademarks with Software License

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.

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.

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)

© 2022–2024 Cisco Systems, Inc. All rights reserved.