Release Notes for Cisco IOS XE Catalyst SD-WAN Devices, Cisco IOS XE Catalyst SD-WAN Release 17.10.x

First Published: 2022-11-10

Last Modified: 2023-03-03

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

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 17.10.1a

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 17.10.1a, which provides Cisco 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 SD-WAN Control Components, refer to Release Notes for Cisco SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.10.x

What's New for Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

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

Cisco is constantly enhancing the 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 Release 17.10.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started Guide	
Updates to the SD-AVC Cloud Connector Login Process	Logging in to the Cloud Connector now requires a cloud gateway URL and a one-time password (OTP) instead of a client ID and client secret.

Feature	Description
Cisco Catalyst SD-WAN Systems and Interfaces	
Security Feature Profile in Configuration Groups	This feature allows you to configure Security Profile in the Configuration Groups.

Localized Policy Configuration for QoS, ACL, and Route Features	This feature allows you to configure Policy Object Profile in the Configuration Groups.
	The following enhancements are introduced in the Policy Configuration Group feature.
	• Policy Object Profiles
	  • AS Path
	  • Standard Community
	  • Expanded Community
	  • Data Prefix
	  • Extended Community
	  • Class Map
	  • Mirror
	  • Policer
	  • Prefix
	  • VPN
	• QoS MAP Policy under Service and Transport profiles
	• Route Policy under Service and Transport profiles
	• ACL Policy under Service and Transport profiles

Variables and Type6 Encryption in CLI Profile	After you enter or import configuration into a CLI profile, convert certain values to device-specific variables or encrypt strings such as passwords using Type6 encryption.
Secure SRST support on Cisco Catalyst SD-WAN	This feature provides support for additional CUBE commands that can be used in Cisco IOS XE Catalyst SD-WAN device CLI templates or CLI add-on feature templates, and qualifies selected Cisco Survivable Remote Site Telephony (SRST) commands for use with CLI templates in Cisco SD-WAN Manager.
DHCP Vendor Option Support	This feature allows DHCP client options, 124 and 125 to configure vendor-specific information in client-server exchanges. Configure this feature using the CLI Add-on feature template in Cisco SD-WAN Manager.

Feature	Description
IPv6 as Preferred Address Family in a Dual Stack Environment	This feature allows you to select IPv6 as the preferred address family for control and data connections in a dual stack network environment. For Cisco SD-WAN Manager and Cisco Catalyst SD-WAN Controller, configure IPv6 as the preferred address family by using the feature template or the CLI template. For Cisco IOS XE SD-WAN devices, configure IPv6 as the preferred address family using the Configuration Groups, Quick Connect or a CLI template.
Bulk API Rate Limit for a Cisco SD-WAN Manager Cluster	For a Cisco SD-WAN Manager cluster, the rate limit for bulk APIs equals (rate-limit per node) * (number of nodes in the cluster). Cisco SD-WAN Manager distributes bulk API requests among the nodes in the cluster. With these changes, you can retrieve data faster from a Cisco SD-WAN Manager cluster through bulk APIs.
Network Hierarchy and Resource Management (Phase II)	The following enhancements are introduced in the Network Hierarchy and Resource Management feature. • Creation of a system IP pool on the **Configuration** > **Network Hierarchy** page • Automatic assignment of site ID, system IP, and hostname to a device in the Quick Connect workflow • Display of detailed information on the **Configuration** > **Network Hierarchy** page, including site ID pool, region ID pool, and the list of devices associated with a site
Cisco Catalyst SD-WAN Routing	
Automatically Suspend Unstable Cisco Catalyst SD-WAN BFD Sessions	With this feature, you can automatically suspend an unstable Cisco Catalyst SD-WAN Bidirectional Forwarding Detection (BFD) session based on flap-cycle parameters or on Service-Level Agreement (SLA) parameters. You can also monitor the suspended BFD sessions and manually reset suspended BFD sessions.
Cisco Catalyst SD-WAN Policies	
Flexible NetFlow Export of BFD Metrics	With this feature, you can export Bidirectional Forwarding Detection (BFD) metrics to an external collector for generating BFD metrics of loss, latency, and jitter. This feature provides enhanced monitoring and faster collection of network state data. After you enable export of BFD metrics, configure an export interval for exporting the BFD metrics.
Real-Time Device Options for Monitoring Cflowd and SAIE Flows	With this feature, you can apply filters for monitoring specific Cflowd and Cisco Catalyst SD-WAN Application Intelligence Engine (SAIE) applications or application families running within a VPN on the selected Cisco IOS XE Catalyst SD-WAN device. Real-time device options for monitoring Cflowd and SAIE flows are available on Cisco vEdge devices. This release provides support for monitoring Cflowd and SAIE applications on Cisco IOS XE Catalyst SD-WAN devices.

Feature	Description

Lawful Intercept 2.0 Enhancements	• Cisco SD-WAN Manager GUI enhancements:
	  • A **Sync to vSmart** button to synchronize a newly created intercept configuration with the Cisco Catalyst SD-WAN Controller.
	  • A toggle button to enable or disable an intercept.
	  • A progress page to display the status of the synchronization and activation.
	  • A red dot on the Task-list icon in the Cisco SD-WAN Manager toolbar to indicate any new Lawful Intercept tasks.
	  • A Task list side bar to view a list of active and completed Lawful Intercept tasks.
	  • An intercept retrieve option **Get IRI** to retrieve key information or Intercept Related Information (IRI) from the Cisco Catalyst SD-WAN Controller.
	• Ability to troubleshoot Cisco SD-WAN Manager and Cisco SD-WAN Manager using the debug logs and using admin tech files.

Cisco Catalyst SD-WAN Security	
Cisco Catalyst SD-WAN Identity-Based Firewall Policy Enhancement for SGT Integration	The Cisco Catalyst SD-WAN identity-based firewall policy feature is enhanced to support Security Group Tag (SGT) integration with ISE. SGTs are assigned in networks to simplify policy configuration across devices.
IPS Custom Signature and Offline Updates	This feature lets you download UTD signature packages for the Intrusion Prevention System (IPS) out of band from Cisco.com and upload these packages to Cisco SD-WAN Manager or a remote server for Cisco SD-WAN Manager to distribute. It also lets you upload a custom signature rules file to Cisco SD-WAN Manager or a remote server, which Cisco SD-WAN Manager then distributes and appends to the existing UTD signature package rules.
Configure SIG Tunnels in a Security Feature Profile	With this feature, create a Security feature profile and associate it with one or more configuration groups. In the Security feature profile, configure the Secure Internet Gateway feature to create automatic or manual SIG tunnels. After configuring the feature, deploy the configuration group on the desired WAN edge devices to create SIG tunnels from the devices to the configured SIG endpoints.
Configure Multiple IdPs for Single Sign-On Users of Cisco SD-WAN Manager	With this feature, you can configure up to three IdPs for providing different levels of access for single sign-on users of Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN Cloud OnRamp	

Feature	Description
Improved Visibility and Control of Webex Traffic	This feature introduces several improvements to the visibility and control of Webex traffic, including the following: • Using Cisco SD-AVC to manage deep packet inspection (DPI) of Webex traffic • Receiving server-side Webex metrics to provide detailed information about Webex traffic performance • Adding only a single sequence to control policies to enable Cloud OnRamp for SaaS for Webex traffic
Monitoring MultiCloud Services for Real Time Data in Cisco SD-WAN Manager	This feature provides enhancements to monitoring dashboard for all the Cloud and Interconnect connections. This feature also gives you the flexibility to specify which dashlets to view and sort them based on your preferences.
Modify Additional Properties of Interconnect Connections to AWS and Microsoft Azure	Interconnect Connections to AWS: • Cisco vManage Release 20.9.x and earlier: You can edit only the bandwidth of a hosted VIF connection after it is created. Properties of hosted connections cannot be edited after connection creation. With this feature, edit additional properties of both hosted VIF and hosted connections after connection creation. • Cisco vManage Release 20.9.x and earlier: You cannot edit a VPC tag that is associated with a connection. With this feature, to attach VPCs to or detach VPCs from a Private Hosted VIF, Private Hosted Connection, or a Transit Hosted Connection, edit the VPC tags associated with the connection to add or remove VPCs. Interconnect Connections to Microsoft Azure: • Cisco vManage Release 20.9.x and earlier: You can edit only the bandwith of a connection after it is created. Other properties of a connection are not editable. With this feature, edit additional properties of both Microsoft peering and private peering connections. • Cisco vManage Release 20.9.x and earlier: You cannot edit a VNet tag that is associated with a connection. With this feature, to attach VNets to or detach VNets from a Private Peering Connection, edit the VNet tags associated with the connection to add or remove VNets.
Cisco Catalyst SD-WAN Monitor and Maintain	
Applications Performance and Site Monitor	You can monitor and optimize the application health and performance on all sites or a single site using Cisco SD-WAN Manager.

Feature	Description
Reports	Reports provide a summarized view of the health and performance of the sites, devices, and tunnels in your network. You can schedule a report, download it as a PDF document, and receive it as an email. The **Reports** menu has been added to Cisco SD-WAN Manager.
Remote Server Support For ZTP Software Upgrades	This features introduces remote server support for upgrading the software of the Cisco IOS XE Catalyst SD-WAN Devices in scale using Zero Touch Provisioning (ZTP). The software upgrade images are uploaded to Cisco SD-WAN Manager using a preferred remote server and the respective devices are upgraded.
Improved Access to Troubleshooting Tools in Cisco SD-WAN Manager	The troubleshooting tools are now easily accessible from various monitoring pages of Cisco vManage, such as **Site Topology**, **Devices**, **Tunnels**, and **Applications**, thereby providing you context-based troubleshooting guidance. Earlier, the troubleshooting tools were accessible only from the device dashboard.
Speed Test Support	This feature enables you to carry out speed testing and evaluate the bandwidths on Cisco IOS XE Catalyst SD-WAN devices and iperf3 servers.
Time Filter in Monitor Overview and Monitor Security Dashboards in Cisco vManage	The time filter option added to the **Monitor Overview** and **Monitor Security** dashboards in Cisco SD-WAN Manager enables you to filter the dashboard data for a specified time range.
Underlay Measurement and Tracing Services	The underlay measurement and tracing services (UMTS) feature provides visibility into the paths that tunnels take between local and remote Cisco IOS XE Catalyst SD-WAN Devices, through the underlay network (the physical devices that compose the network). For a specific tunnel, the path includes all nodes between the two devices. You can enable UMTS using Cisco SD-WAN Manager. You can view the resulting path information in Cisco SD-WAN Manager and in Cisco vAnalytics.
Software Upgrade Scheduling Support for Additional Platforms	Added support for software upgrade scheduling for Cisco Catalyst Cellular Gateways and Cisco Catalyst Wireless Gateways.
Cisco Catalyst SD-WAN NAT	
Support for Source Port Preservation for well-known SD-WAN Ports	This feature allows preservation of well-known SD-WAN ports during NAT.
Mapping of Address and Port Using Encapsulation (MAP-E) with NAT64	This feature provides support for an IPv4 client to access IPv4 servers when using an IPv6-only network. IPv4 traffic is routed to the internet over an IPv6 tunnel. With this feature, you can configure a MAP-E domain and MAP-E parameters for transporting IPv4 packets over an IPv6 network using IP encapsulation. When the MAP-E customer edge (CE) device starts or when an IPv4 address changes, the device obtains the MAP-E parameters automatically from the MAP-E rule server using HTTP.
Cisco Catalyst SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN)	

Feature	Description
Multi-Region Fabric Subregions	You can create subregions within an access region. Subregions enable you to separate edge routers into multiple distinct domains.
Multi-Region Fabric Using Multicloud and SDCI	This feature enables you to configure a cloud backbone or a Software-Defined Cloud Interconnect (SDCI) provider backbone as core region (region 0), and cloud gateways or interconnect gateways as border routers. You can thus easily establish site-to-site connectivity in multiple cloud regions and cloud networks.
Subregions in Policy	Subregions are defined domains within access regions. You can specify subregions when creating region lists, configuring policy, and applying policy.
Enhancements to Match Conditions	When configuring match conditions for policy, you can specify to match to all access regions, or to match according to a subregion.
Migrate a BGP-Based Hierarchical Core Network to Multi-Region Fabric	This feature facilitates migrating a BGP-based hierarchical core network into a Cisco 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 CloudOps	
Multitenancy Support on Microsoft Azure	Multitenancy Support for Cisco SD-WAN Control Components on Microsoft Azure.
Cisco IOS XE Catalyst SD-WAN Qualified Command Reference	
CLI Hardening Commands on Cisco IOS XE SD-WAN devices	CLI Hardening commands are added in AAA Commands Line Commands Logging Commands SNMP Commands

New and Enhanced Hardware Features

New Features

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

- Cisco ISR 4000 Series Integrated Services Routers:
  - ISR 4461
  - ISR 4451
  - ISR 4351
  - ISR 4431

- Cisco Catalyst 8300 Series Edge Platforms:
  - C8300-2N2S-4T2X
  - C8300-2N2S-6T
  - C8300-1N1S-4T2X
  - C8300-1N1S-6T

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

Table 2: Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

Behavior Change	Description
On the **SD-AVC Cloud Connector** page, the **Category** field is renamed in the table displaying information about Microsoft Office 365 traffic, and the table includes a new **Geography** field.	The View Office 365 Server Information Using the SD-AVC Cloud Connector section shows the new field and field name.
A **show sdwan from-vsmart commit-history** command is added for verifying policy-related commit events and for analyzing the average time required for the policy commit.	A new command, show sdwan from-vsmart commit-history, is added.
The **request software activate** command no longer supports the **clean** option for activating the specified software image without associating the existing configuration file or files that store information about the device history.	The request software activate command no longer supports the **clean** option.

Behavior Change	Description
The "Cisco Systems" string is added in the Organization Names list along with "vIPtela Inc" or "Viptela LLC" strings.	The Enable Reverse Proxy section has the new acceptable organization name for the enterprise certificates.
Cisco Catalyst SD-WAN Cloud Interconnect with Megaport is supported only on versions Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later.	The section Restrictions for for Catalyst Cisco SD-WAN Cloud Interconnect with Megaport has the new restriction on the supported versions.
A new service container **device-data-collector** is added to start, stop and diagnose the NMS services.	The Manually Restart SD-WAN Manager Processes section is updated with new container details.
If Cisco SD-WAN Manager is running Cisco vManage Release 20.7.1 and Cisco vManage Release 20.8.1, a direct update to Cisco vManage Release 20.10.1 is not supported. Cisco vManage needs to run Cisco vManage Release 20.9.1.	A note is added to the Important Notes, Known Behaviors, and Workarounds section in the Release Notes for Cisco Catalyst SD-WAN Control Components, Cisco Catalyst SD-WAN Control Components Release 20.10.x.
The **Decrement Value** field in the SVI Interface feature is now enabled only when you choose **decrement** in the **Track Action** field.	A note is added in the SVI Interface section.

Behavior Change	Description
The **Community Name** field has been removed from the SNMP feature. In its place, the **User Label** field has been added that helps you distinguish or update a community name when there are multiple community names for an SNMP target.	The new **User Label** field is described in the SNMP section. Similarly, a note is added for the **Community Name** field.
To create or update a CLI add-on profile, you must have appropriate permission for the CLI Add-On Template feature.	A note is added in the CLI Profile section.
An **Internet Outages** option is added to the **Analytics** menu in Cisco SD-WAN Manager.	The **Internet Outages** option is described in the Internet Outages section.

Important Notes, Known Behaviors, and Workarounds

- Cisco IOS XE Catalyst SD-WAN devices with the SFP-10G-SR module do not support online insertion and removal (OIR) of this module.
- Cisco vManage Release 20.3.1 implements a hardened security posture to comply with FedRamp guidelines. As a result, your vAnalytics login credentials that are stored locally get erased on upgrading the software, and you cannot access the Cisco SD-WAN Analytics service directly through Cisco SD-WAN Manager. In this case, log in to Cisco SD-WAN Analytics using this URL: https://analytics.viptela.com. If you can't find your Cisco SD-WAN Analytics login credentials, open a case with Cisco TAC support.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, the **`table`** keyword is added to all show sdwan commands for which the output needs to be displayed in a tabular format. Using **`| tab`** is restricted for all Cisco Catalyst SD-WAN commands starting from Cisco IOS XE Catalyst SD-WAN Release 16.11.x.
- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, feature templates support the following network interface modules for Layer 3 features:
  - Cisco 2-port 100-Mbps/1-Gbps WAN Network Interface Module with 256-bit WAN MACsec (C-NIM-2T)
  - Cisco 1-port 2.5-Gbps/1-Gbps WAN Network Interface Module with Cisco UPoE (C-NIM-1M)

- Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, the Switch Port feature template supports an interface speed of 2500 Mbps when configuring a 2-Gigabit Ethernet interface for the following modules:
  - Cisco SM-X-16G4M2X and Cisco SM-X-40G8M2X EtherSwitch Service Modules on Cisco ISR 4000 Series Routers
  - Cisco C-SM-16P4M2X and Cisco C-SM-40P8M2X EtherSwitch Service Modules on Cisco Catalyst 8300 Series Edge Platforms
- **Cloud OnRamp for IaaS**: Beginning with Cisco vManage Release 20.9.1, we recommend setting up your cloud infrastructure using Cloud OnRamp for Multicloud. Cloud OnRamp for IaaS will be phased out in a future release.
- Beginning with Cisco vManage Release 20.9.1, you can add the route-target CLIs through the CLI add-on profile of a configuration group:

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

- When you configure a PPPoE dialer interface with NAT DIA enabled, the ppp chap password considers the default value as 7.

Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.10.x

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 17.10.1a

Identifier	Headline
CSCwd56015	UTD skipped when interface UTD config is used to enable/disable UTD
CSCwc76082	"check_sig_ipsec_ike_sessions" fails with could not find entry for Tunnel100001
CSCwd56336	BFD sessions are not coming up after flapping the interface due to low ftm rate
CSCwb90533	OMPD Daemon crashed while doing show command
CSCwd15560	With 2 sequences, should not skip if the match is different and action is same
CSCwc77621	SNMP auth failures due to out of sync snmp community string
CSCwd71656	17.10 Auto GRE- After reboot, no ip address assigned to destination address for 1 tunnel
CSCwd12955	NAT translation is not correctly sent to hub router from branch when SSNAT and UTD are configured
CSCwd45894	Cisco Catalyst SD-WAN ACL TCAM not in sync with configuration
CSCwd12591	Cisco ISR4000 Cisco IOS XE Catalyst SD-WAN device - ucode crash during FW Classification, Session Frees

Identifier	Headline
CSCwb32635	17.6.2 IOS XE SD-WAN - vdaemon file is incomplete when running admin-tech
CSCwd13352	SSH from Cisco SD-WAN Manager vshell to Cisco IOS XE Catalyst SD-WAN device getting closed after Cisco IOS XE Catalyst SD-WAN device update.
CSCwd17381	NAT/DIA traffic is skipping UTD in forward direction after SSNAT path from service-side
CSCwd34573	Sparrow crashed: fman_fp_image: QFP0.0 CPP Driver LOCKDOWN encountered due to previous fatal error
CSCwd15070	Cisco IOS XE Catalyst SD-WAN device upgrade fails and can't change template due to "advertise aggregate" config w/o prefix-list
CSCwc77003	Prefix through hub not intalled in FIB, with OD Tunnels, seeing drops due to FirewallPolicy
CSCwc79847	Router Crashed | Last reload reason: Critical process ftmd fault on rp_0_0 (rc=134))
CSCwd14061	FTM is shooting up high and stuck in loop with the function ftm_sa_add().
CSCwd01326	Catalyst 8500L - qfp-ucode-fugazi crashes with SIGABRT within cio infra under heavy load

Open Bugs for Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

Identifier	Headline
CSCwd45508	Cisco IOS XE Catalyst SD-WAN device does not form BFD across Serial link when upgrading from 17.3.3 to 17.6.x
CSCwd63783	Memory leak on vdaemon process caused Cisco IOS XE Catalyst SD-WAN device router reload
CSCwd47940	Cisco IOS XE Catalyst SD-WAN device: PMTU Discovery is not working after interface flap
CSCwd13050	After upgrade to 20.6.3, Cisco IOS XE SD-WAN devices moved into Out of Sync status on Cisco SD-WAN Manager.
CSCwd48781	Cisco IOS XE Catalyst SD-WAN device ASR1k crashed due to Critical process cxpd fault
CSCwc28468	Cisco Catalyst SD-WAN mode: Cisco SD-WAN Manager always fails to push any template to device if device is running in FIPS mode.
CSCwd44439	ASR and c8500 crashing at fman_SD-WAN_nh_indirect_delete_from_hash_table
CSCwd34941	NAT configuration with no-alias option is not preserved after reload
CSCwd33966	Unable to configure the local BGP as-path-list via Cisco SD-WAN Manager.

Identifier	Headline
CSCwc68069	RTP packets not forwarded when packet duplication enabled, no issue without duplication feature
CSCwd37410	0365 and MS Teams applications access issues when using DIA with app-list match in data-policy
CSCwc37465	unable to push "no-alias" option on static NAT mapping from management system
CSCwd47937	Device roll back doesn't work on C1121X-8P on 17.6.3a
CSCwa92817	SNMP polling not working on PPP Interface on ISR1100
CSCwd60313	17.10 - When source interface is changed, ike negotiation is not restarted
CSCwd44006	Control Connection on Cisco IOS XE Catalyst SD-WAN device doesn't come-up with reverse proxy using Enterprise Certificate
CSCwd63999	Bootstrap fails on c1121x due to 802.1x config
CSCwd44586	Cisco Catalyst SD-WAN Cisco IOS XE Catalyst SD-WAN device - Login banner config is changed after upgrade to 17.6.3a
CSCwd57171	OMP not withdrawing route advertisement after OSPF route is removed from RIB
CSCwa14636	Cisco IOS XE Catakyst SD-WAN device stopped forwarding traffic. Suspect OMPd is busy
CSCwc38529	[Cisco IOS XE Catalyst SD-WAN device 17.6] Traffic seems not inspected by UTD when umbrella is set
CSCwc48427	[SITLite] BFD issues with clear_omp -> non-PWK + non-VRRP scenario only
CSCwd59870	Centralized Data Policy "From-Tunnel" not forwarding traffic to next hop
CSCwd53506	Login authentication default is not recognize on lines VTY
CSCwd89012	Tested flap-based auto-suspension - minimum duration value - no results as expected

Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations

For compatibility information and server recommendations, see Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations.

Supported Devices

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

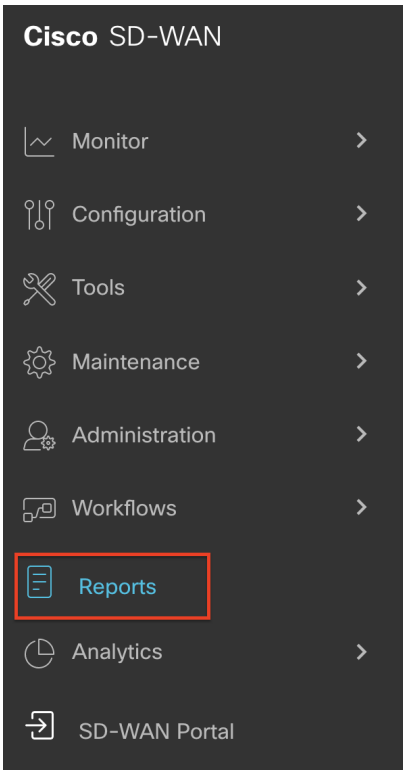
Cisco SD-WAN Manager GUI Changes

This section presents a comparative summary of the significant GUI changes between Cisco vManage 20.9.x and Cisco vManage Release 20.10.1.

Reports Menu

In Cisco vManage Release 20.10.1, the **Reports** menu has been added to Cisco SD-WAN Manager. For more information about reports, see Reports.

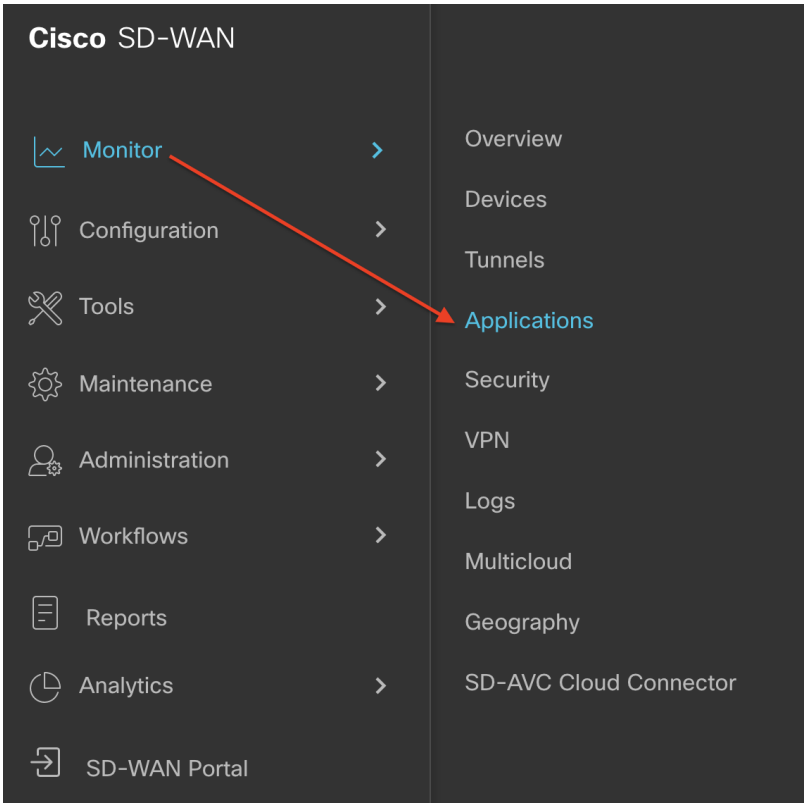
Figure 1: Reports Menu in Cisco SD-WAN Manager 20.10.1



Applications Submenu

In Cisco vManage Release 20.10.1, the **Applications** submenu has been added to the **Monitor** menu in Cisco SD-WAN Manager. For more information about the **Applications** submenu, see Applications Performance and Site Monitor.

Figure 2: Applications Submenu in Cisco SD-WAN Manager 20.10.1

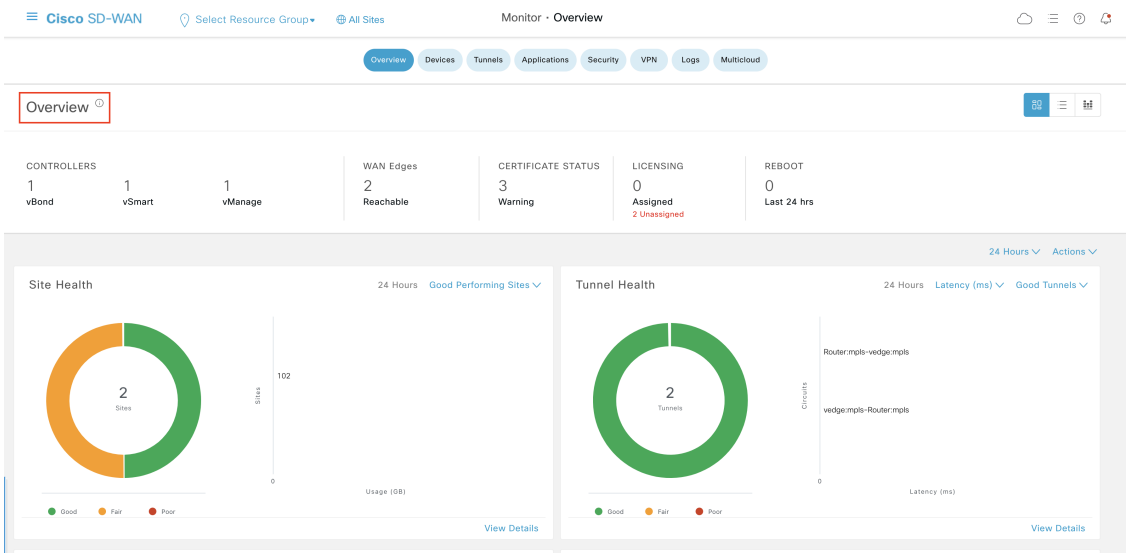


Monitor Overview Page

In Cisco vManage Release 20.10.1, the following GUI changes have been made to the **Monitor** > **Overview** page. For more information about the **Monitor** > **Overview** page, see Cisco SD-WAN Manager Monitor Overview.

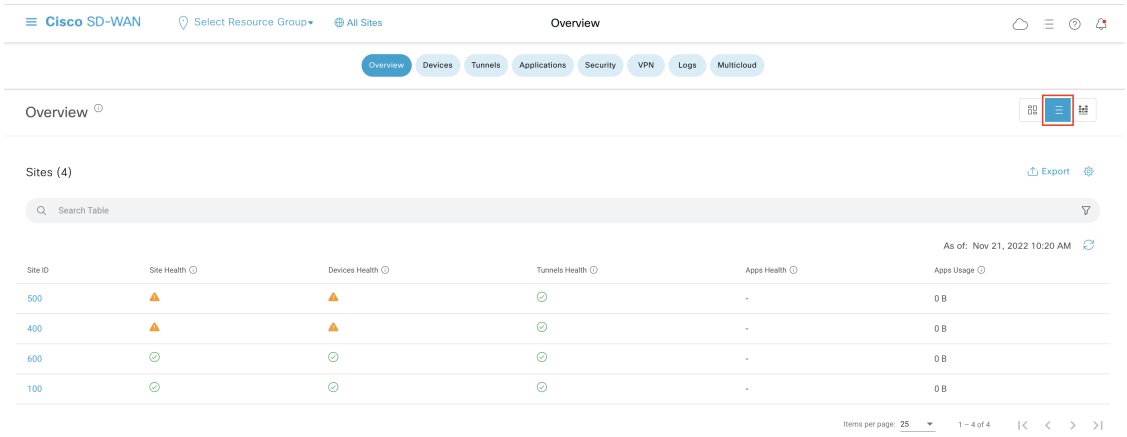
- The page title, **Overview**, and an infotip have been added.

Figure 3: Monitor Overview Page Title and Infotip in Cisco SD-WAN Manager 20.10.1



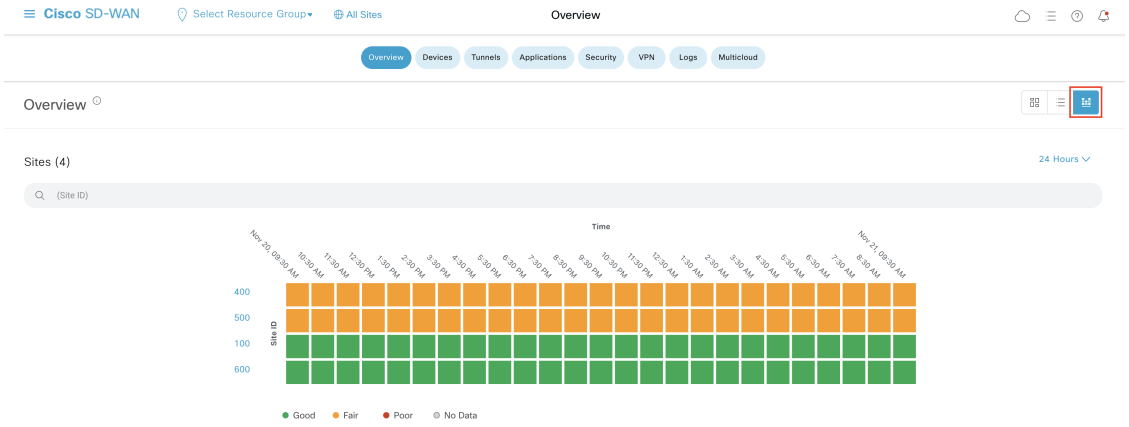
- The table view has been added to the page.

Figure 4: Table View of the Monitor Overview Page in Cisco SD-WAN Manager 20.10.1



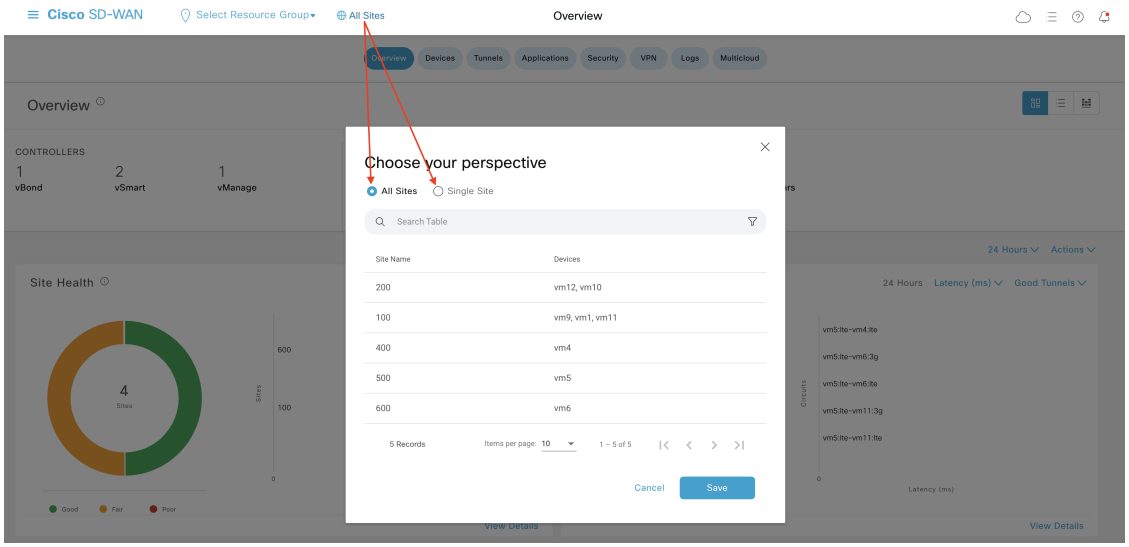
- The heat map view has been added to the page.

Figure 5: Heat Map View of the Monitor Overview Page in Cisco SD-WAN Manager 20.10.1



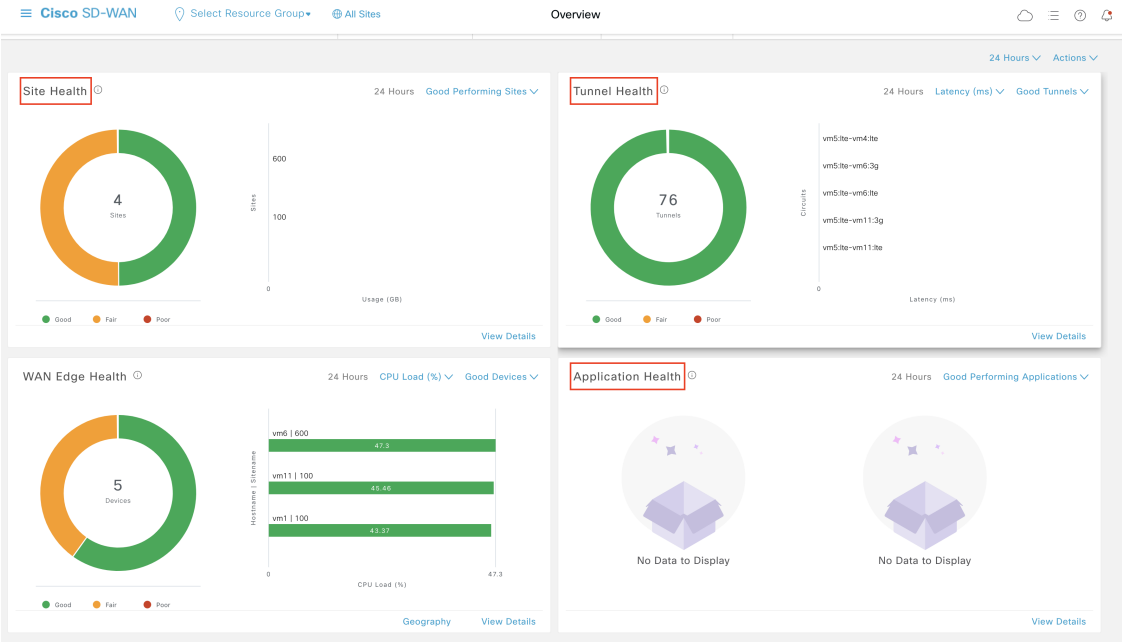
- The site selection option has been added to the page.

Figure 6: Site Selection Option in the Monitor Overview Page in Cisco SD-WAN Manager 20.10.1



- Three new dashlets, **Site Health**, **Tunnel Health**, and **Application Health** have been added.

Figure 7: New Dashlets in the Monitor Overview Page in Cisco SD-WAN Manager 20.10.1



- The **WAN Edge Health** dashlet has been updated.

Figure 8: WAN Edge Health Dashlet in the Monitor Overview Page in Cisco SD-WAN Manager 20.9.x

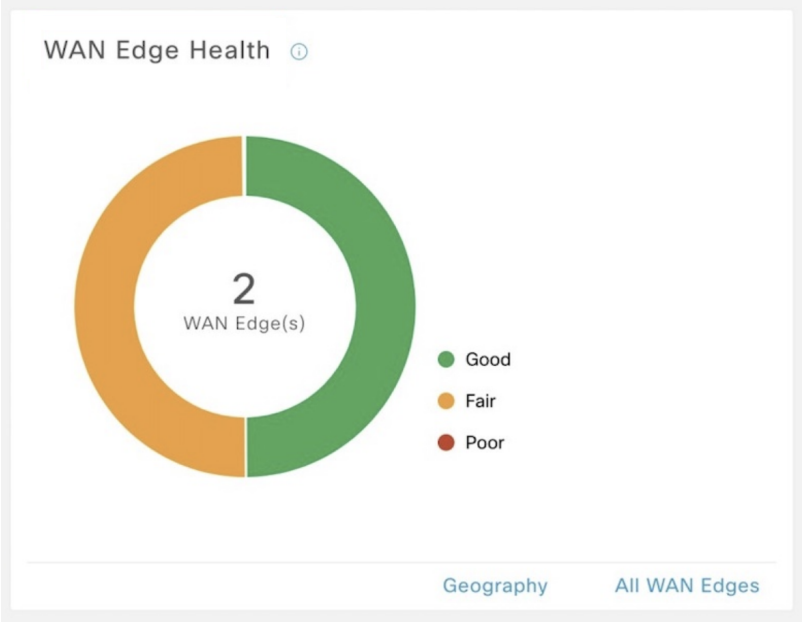
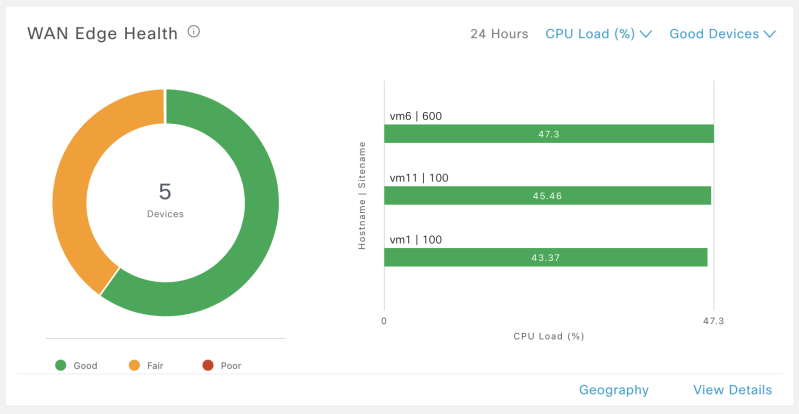


Figure 9: WAN Edge Health Dashlet in the Monitor Overview Page in Cisco SD-WAN Manager 20.10.1

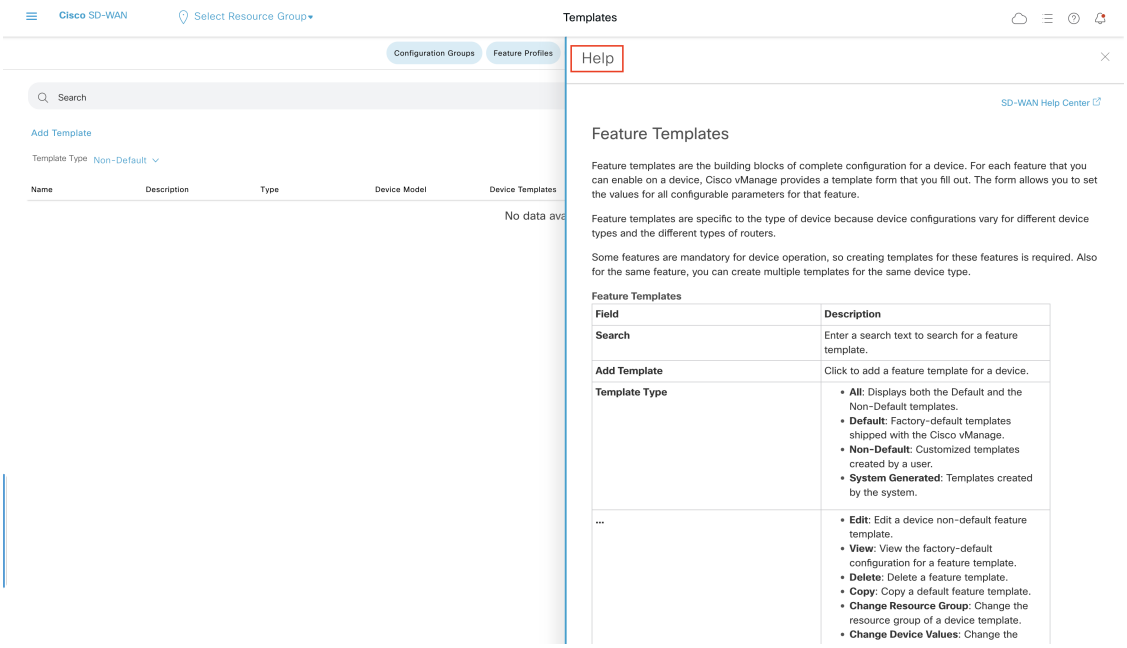


In-product Help

In a single-tenant deployment, access help content for Cisco SD-WAN Manager UI pages by clicking the **Help** icon at the top-right corner of a page. The help content is displayed in a slide-in pane in the same browser window.

Starting from Cisco SD-WAN Manager Release 20.12.x, In-product help is available for a majority of the Cisco SD-WAN Manager UI pages.

Figure 10: Help Content in a Slide-in Pane



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.

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)

© 2022–2023 Cisco Systems, Inc. All rights reserved.