Release Notes for Cisco Catalyst SD-WAN Control Components Release 20.14.x

First Published: 2024-04-30

Read Me First

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

Related References

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

User Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17
- User Documentation for Cisco SD-WAN Release 20

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.

- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

Release Notes for Cisco SD-WAN Control Components, Cisco Catalyst SD-WAN Manager Release 20.14.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 20.14.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 Release 17.14.x.

What's New for Cisco Catalyst SD-WAN Manager Release 20.14.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.

Table 1: Cisco Catalyst SD-WAN Manager Release 20.14.1

Feature	Description
Cisco Catalyst SD-WAN Getting Started	
Cisco SD-WAN Manager Cluster Upgrade Compatibility Check	This feature helps to upgrade Cisco SD-WAN Manager cluster and ensures that all the software devices are running on same version and are compatible. Using this feature, you can check pre-upgrade and post-upgrade checks to verify node health and identify the cause for inconsistent failures.

Feature	Description
Support for Disk Encryption in On-Premises ESXi for a Virtual Machine Hosting Cisco SD-WAN Control Components	With this feature, you can apply disk encryption on the virtual disk when hosting Cisco SD-WAN Control Components in an on-premises installation, using a VMWare ESXi hypervisor hosted on a Cisco UCS platform.
Cisco Catalyst SD-WAN Monitor and Maintain	
Security Dashboard Enhancements	The following enhancements have been made to the security dashboard in Cisco SD-WAN Manager: • A new **Security Appliance/UTD Container** dashlet has been added to monitor the health status of the Firewall and UTD components, such as the Cisco Intrusion Prevention System (IPS), Advanced Malware Protection (AMP), and Cisco URL filtering. • A new **Application Offload** dashlet has been introduced that displays the breakdown of application traffic across SIG/SEE Tunnels and Direct Internet Access (DIA), and provides more details about the application traffic. • Updates have been made to the existing dashlets to provide more detailed information about Events. • Navigate from the Intrusion Prevention dashlet to the Talos website to view Snort rules.
Improved Monitoring of Cellular-Enabled Devices	Cisco SD-WAN Manager provides detailed information about the connectivity of cellular-enabled devices, and the health of the connections, to provide a holistic view of cellular connectivity health. In addition, you can filter the device list to specifically display cellular-enabled devices, among other filter options.
Cisco Catalyst SD-WAN System and Interfaces	
Multitenancy Support for Cisco Catalyst Cellular Gateways	Added multitenancy support for Cisco Catalyst Cellular Gateways.
CMAC-AES-128 Authentication for NTP Servers	Support for cipher-based message authentication code (CMAC) advanced encryption standard (AES) 128-bit (cmac-aes-128) authentication for network time protocol (NTP) server configuration for Cisco SD-WAN Control Components.

Table 2: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

Feature	Description
Cisco Catalyst SD-WAN Getting Started	

Feature	Description
New Procedure for Enabling Cisco SD-AVC Cloud Connector	This release introduces a new procedure for enabling Cisco SD-AVC Cloud Connector from the Cloud Services option in **Administration** > **Settings**. From this release, enabling Cloud Connector does not require an OTP or opening a TAC case.
Cisco SD-WAN Manager Cluster Upgrade Compatibility Check	This feature helps to upgrade Cisco SD-WAN Manager cluster and ensures that all the software devices are running on same version and are compatible. Using this feature, you can check pre-upgrade and post-upgrade checks to verify node health and identify the cause for inconsistent failures.
License Compliance Messaging	Cisco SD-WAN Manager actively monitors the compliance status of Cisco Catalyst SD-WAN licenses to identify issues with license synchronization, device assignments, or expired licenses. In case of an issue, it displays a compliance error message. In addition, on the **License Management** page, the device list indicates the license compliance status of each device.
Release a License from a Device	You can manually release a license from a device without having to remove or decommission the device. This leaves the license available to use with other devices.
Multitenant License Management	In a multitenant scenario, Cisco SD-WAN Manager supports license management at the provider level for multitenant edge devices. In Cisco SD-WAN Manager, in Provider mode, assign a base license and tenant licenses for multitenant edge devices.
Cisco Catalyst SD-WAN Security	
Match Traffic Using Custom Applications	Added support for matching traffic using a custom application in a custom-defined application list.
IPv6 Support for UTD policies	This feature adds IPv6 support for UTD security features and Unified Logging. IPv6 support for UTD security feature includes configuration and inspection of IPv6 traffic, IPS, URL filtering, and AMP. The feature also adds IPv6 support for operational command related to UTD.
SLA Profile support for Layer 7 Health Check	This feature uses jitter and packet loss, in addition to latency in SLA metrics to determine the health of the tunnel.
Zscaler Integration	This feature adds Zscaler integration with Cisco Catalyst SD-WAN as a Security Service Edge (SSE) solution. You can provision both IPSec and GRE tunnels to Zscaler using policy groups in Cisco SD-WAN Manager.
IPv6 GRE or IPsec Tunnels Between Cisco IOS XE Catalyst SD-WAN and Third-Party Devices over a transport VPN	This feature allows you to configure an IPv6 GRE or IPSEC tunnel from a Cisco IOS XE Catalyst SD-WAN device to a third-party device over a transport VPN.
Cisco Catalyst SD-WAN Cloud OnRamp	

Feature	Description
Configure Devices for AWS Integration Using Configuration Groups	This feature enables the use of configuration groups on Cisco SD-WAN Manager to configure devices for AWS integration.
Configure Devices for Azure for US Government Using Configuration Groups	This feature enables the use of configuration groups on Cisco SD-WAN Manager to configure devices using automation for Azure for US Government.
Pay As You Go and IP-Transit License Management for Megaport	This feature introduces support for Pay As You Go (PAYG) licenses for Megaport. The PAYG model is a usage-based model which allows users to pay based on how much they consume. For example, a cloud storage service provider could charge based on the amount of storage used.
Cisco Catalyst SD-WAN AppQoE	
IPv6 Protocol support for AppQoE Services	This feature allows AppQoE clusters to handle both IPv4 and IPv6 traffic.
DRE Optimization Using Configuration Groups	With this feature you can enable DRE optimization using **AppQoE** feature under **Service Profile** in a configuration group in Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN Monitor and Maintain	
Cellular Modem Firmware Upgrade	Cisco SD-WAN Manager supports upgrading the cellular modem firmware of devices that include a cellular modem.
Protocol Pack Management and Compliance	Cisco SD-WAN Manager management of Protocol Packs includes upgrading Protocol Pack releases on routers in the network and flagging the status of routers using an older Protocol Pack release than the current reference release. Cisco SD-WAN Manager uses the latest Protocol Pack release that it has available as a reference for comparing against the Protocol Packs loaded on devices in the network.
Export and Import Cisco Catalyst SD-WAN Configurations	Export and import configuration groups, policy groups and toplogies from your Cisco SD-WAN Manager as .tar.gz files to your local storage and customize your deployments.
Cisco Catalyst SD-WAN System and Interfaces	
L2VPN Support on Cisco Catalyst SDWAN Overlay	The feature adds Layer 2 VPN support on the Cisco Catalyst SD-WAN overlay network. It allows you to configure Layer 2 point-to-point and point-to-multipoint connections within the Cisco Catalyst SD-WAN fabric.

Feature	Description
Support for Load Balancing for EtherChannels on the Transport Side	This feature adds the ability to configure load balancing for EtherChannels on the transport side for Cisco IOS XE Catalyst SD-WAN devices using the **port-channel load-balance-hash-algo sdwan** command.
Cisco Catalyst SD-WAN Rugged Series Router Configuration Guide	
Configure WIM on Cisco Catalyst IR1800 Rugged Series Routers	Configure and manage the Wi-Fi Interface Module (WIM) on Cisco Catalyst IR1800 Rugged Series Routers using Cisco SD-WAN Manager.
Cisco Catalyst SD-WAN NAT	
Support for configuring multiple NAT types	This feature supports configuration of multiple NAT types - interface, loopback interface, or NAT pool for Direct Internet Access (DIA). Use the centralized data policy to assign rules for combining various NAT types for DIA traffic egressing the Edge router. You can also bypass NAT altogether.
Support for redistribution of NAT66 DIA routes	You can configure the redistribution of NAT66 DIA routes into BGP or OSPFv3 protocols.
Support for NAT66 DIA status event.	You can monitor the NAT DIA status in the Cisco SD-WAN Manager logs. A new event called **nat-update** displays the status of NAT DIA in the **Events** screen.
Support for Point-to-Point Protocol (PPP) Dialer Interfaces with NAT66 DIA	This feature adds support for two types of PPP dialer interfaces—PPP over Ethernet (PPPoE) and PPP over Asynchronous Transfer Mode (PPPoA). With this feature, you can configure PPP dialer interfaces for accessing IPv6 services and sites.
Cisco Catalyst SD-WAN Remote Access	
Monitor Cisco Catalyst SD-WAN Remote Access using Cisco SD-WAN Manager	The feature enhances the monitoring of remote access devices. Cisco SD-WAN Manager can provide the following information: Number of remote access (RA) headends in the network and the supported RA mode (IPsec/SSLVPN). Number of remote access sessions in the network and sessions per remote access headend categorized into remote access client type.
Policies	
Service Chaining Trusted and Untrusted Traffic	This feature lets you configure trusted traffic to flow to a trusted high availability pair in a service chain.

Feature	Description
Configure a Maximum FNF Record Rate for Aggregated Traffic Data	For a device, you can configure a maximum rate (records per minute) for sending Flexible NetFlow (FNF) records of aggregated traffic data. This can reduce the performance demands on a device, and may be helpful when there is a large number of applications producing network traffic.
Policy Groups	
Policy Compliance	This feature checks whether existing application-aware policies use applications that have been updated in a later Protocol Pack, and assists you in updating policies to use the latest available applications. The compliance-check uses the Protocol Pack currently loaded in Cisco SD-WAN Manager as a reference.
Cisco Catalyst SD-WAN Configuration Groups	
Support for Additional OK Communications Features	This feature adds support for the Unified Voice configuration features in the UC voice profile.
Network-Wide Path Insight	
Network-Wide Path Insight Integration with Cisco ThousandEyes	With this feature, network-wide path insight presents test results from a Cisco ThousandEyes Enterprise Agent and includes this information in flow results for your review and analysis.
Qualified Command Reference	
Event Commands	The EEM configurations such as else, break, continue, elseif, while, set, increment, handle-error, gets, foreach, divide, decrement, counter, and append are supported.

Software and Hardware Behavior Changes in Cisco Catalyst SD-WAN Control Components Release 20.14.x

Software and Hardware Behavior Changes in Cisco Catalyst SD-WAN Manager Release 20.14.1

Behavior Change	Description
The Cisco Catalyst SD-WAN Manager Release 20.14.1 software image names are renamed from viptela-edge to viptela-bond. The Cisco vBond component is renamed to Cisco SD-WAN Validator in the new software versions. The vEdge Cloud is not supported from Cisco Catalyst SD-WAN Control Components Release 20.9.1. A unified software image is used for Cisco SD-WAN Controller (vSmart) and Cisco SD-WAN Validator (vBond). The initial default hostname for both controllers is vsmart. We recommended you to update the hostname.	See the Download Software section for more information about Cisco SD-WAN Validator changes.

Software and Hardware Behavior Changes in Cisco IOS XE Catalyst SD-WAN Release 17.14.1a

Behavior Change	Description
The SLA class components such as loss, latency and jitter values are modified.	The Application Priority and SLA section describes the new SLA class component values.
The **request platform software sdwan software activate** is updated with supported options.	The request platform software sdwan software activate command is updated.
In an environment that mixes Cloud OnRamp for SaaS without SIG tunnels and Cloud OnRamp for SaaS over SIG tunnels, telemetry is supported for sites using Cloud OnRamp for SaaS without SIG.	The Restrictions for Cloud OnRamp for SaaS Over SIG Tunnels section describes the details.
From Cisco SD-WAN Manager, the auto correct option is not available. Instead, display the cloud services audit as follows: From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**, then in the **Intent Management** pane, click **Audit**. Select the cloud provider. Cisco SD-WAN Manager shows the audit report.	The Audit Discrepancies and Resolutions table provides more details.
Advertisement of NAT64 routes through OMP is supported through Cisco IOS XE Catalyst SD-WAN Release 17.12.x.	The Advertise NAT64 Routes Through OMP section is updated.
When a Cisco SD-WAN Controller or Cisco SD-WAN Validator upgrade is in progress, upgrade of tenant edge devices is not supported.	The Restrictions for Cisco Catalyst SD-WAN Multitenancy section describes the details.

Behavior Change	Description
AppQoE clusters can handle both IPv4 and IPv6 traffic for TCP and DRE optimization.	The Create a Centralized Policy for TCP and DRE Optimization section describes the details.
In Cisco SD-WAN Manager, the **Data Collection** tab has been removed from **Administration >** > **Settings** and integrated into **Network Statistics Configuration and Collection**, and a new tab **Terms & Conditions** now has these two toggle options for collecting telemetry data, **SD-WAN Telemetry Basic** and **SD-WAN Telemetry Advanced**.	The Data Collection and Cisco Catalyst SD-WAN Telemetry section describes the details.

Important Notes, Known Behaviors, and Workarounds

- To improve the performance of statistics processing, this release incorporates improvements to the Cisco Catalyst SD-WAN architecture. This change improves the Cisco SD-WAN Manager user interface responsiveness, as well as scalability. After upgrading to Cisco Catalyst SD-WAN Manager Release 20.14.x, Cisco SD-WAN Manager requires some time to migrate statistics data. Depending on the volume of data, there may be a delay in loading some of the charts and data on the **Monitor** > **Overview** page. To check the status of the data migration, you can open the Task List and view the migration task.
- From Cisco Catalyst SD-WAN Manager Release 20.14.1, you can navigate to Cisco services hosted in the Cisco Networking Cloud, such as Cisco Spaces, Intersight, IoT Operations Dashboard, Meraki, and Cisco ThousandEyes. Enable the cross platform navigator in **Administration** > **Settings** > **Cross Platform Navigator**.

Cisco Catalyst SD-WAN Manager Upgrade Paths

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

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

Table 3: Upgrade Paths For Cisco Catalyst SD-WAN Control Components Releases 20.6.x and Later Releases

Starting Cisco SD-WAN Manager Version	Destination Version								
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x	20.14.x
20.6.x	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade					

Starting Cisco SD-WAN Manager Version	Destination Version								
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x	20.14.x
					Step upgrade from 20.6.1, 20.6.2, and 20.6.3 either to 20.6.4 or 20.9.x. or Direct upgrade from 20.6.4 and later releases. For cluster upgrade procedure using CLI: **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 from 20.6.1, 20.6.2, and 20.6.3 either to 20.6.4 or 20.9.x. or Direct upgrade from 20.6.4 and later releases. For cluster upgrade procedure using CLI: **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 from 20.6.1, 20.6.2, and 20.6.3 either to 20.6.4 or 20.9.x. or Direct upgrade from 20.6.4 and later releases. For cluster upgrade procedure using CLI: **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 from 20.6.1, 20.6.2, and 20.6.3 either to 20.6.4 or 20.9.x. or Direct upgrade from 20.6.4 and later releases. For cluster upgrade procedure using CLI: **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 from 20.6.1, 20.6.2, and 20.6.3 either to 20.6.4 or 20.9.x. or Direct upgrade from 20.6.4 and later releases. For cluster upgrade procedure using CLI: **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								
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x	20.14.x
20.7.x	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Step upgrade from 20.9.x For cluster upgrade procedure using CLI: **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 from 20.9.x For cluster upgrade procedure using CLI: **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 from 20.9.x For cluster upgrade procedure using CLI: **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 from 20.9.x For cluster upgrade procedure using CLI: **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 from 20.9.x For cluster upgrade procedure using CLI: **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								
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x	20.14.x
20.8.x	Not Supported	Not Supported	Not Supported	Direct Upgrade	Step upgrade from 20.9.x For cluster upgrade procedure using CLI: **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 from 20.9.x For cluster upgrade procedure using CLI: **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 from 20.9.x For cluster upgrade procedure using CLI: **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 from 20.9.x For cluster upgrade procedure using CLI: **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 from 20.9.x For cluster upgrade procedure using CLI: **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								
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x	20.14.x
20.9.x	Not Supported	Not Supported	Not Supported	Not Supported	Direct upgrade For cluster upgrade procedure using CLI: **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 using CLI: **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 using CLI: **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								
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x	20.14.x
								Direct Upgrade For cluster upgrade procedure using CLI: **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. • If your Cisco Catalyst SD-WAN Manager is running Cisco vManage Release	Direct Upgrade For cluster upgrade procedure using CLI: **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. • If your Cisco Catalyst SD-WAN Manager is running Cisco vManage Release

Starting Cisco SD-WAN Manager Version	Destination Version								
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x	20.14.x
								20.9.x and you are looking to upgrade to Cisco Catalyst SD-WAN Manager Release 20.12.x, we recommend you use the CLI mode of configuration for cluster upgrades. If Cisco Catalyst SD-WAN Manager UI is used for upgrading a cluster, the cluster's nms process fails when the new partition is activated. Continue to use the Cisco Catalyst SD-WAN Manager UI and CLI for standalone Cisco SD-WAN Manager upgrades.	20.9.x and you are looking to upgrade to Cisco Catalyst SD-WAN Manager Release 20.12.x, we recommend you use the CLI mode of configuration for cluster upgrades. If Cisco Catalyst SD-WAN Manager UI is used for upgrading a cluster, the cluster's nms process fails when the new partition is activated. Continue to use the Cisco Catalyst SD-WAN Manager UI and CLI for standalone Cisco SD-WAN Manager upgrades.
20.10.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade	Direct Upgrade
20.11.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade	Direct Upgrade

Starting Cisco SD-WAN Manager Version	Destination Version								
	20.6.x	20.7.x	20.8.x	20.9.x	20.10.x	20.11.x	20.12.x	20.13.x	20.14.x
20.12.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade	Direct Upgrade
20.13.x	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Not Supported	Direct Upgrade

Note To check the free disk space using the CLI,

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

Note The cluster upgrade must be performed using CLI,

- The **request nms configuration-db upgrade** upgrade procedure must be performed only on one node in the cluster.
- 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.
- To upgrade the configration database and to determine the node that needs an upgrade, enter **request nms configration-db status** command on each of the nodes. In the output look for the following:

```
Enabled: true
Status: not running
```

Note After activating a new image on a Cisco SD-WAN Manager host server, the server reboots. After the reboot, for approximately 30 minutes, the output of the **request nms configuration-db status** command shows **Enabled: false** even on a node that has the configuration database enabled, while NMS services are being migrated to a containerized form. On the node to upgrade, as determined in the previous step, enter the following: **request nms configration-db upgrade**

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.14.x

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.

Bugs for Cisco Catalyst SD-WAN Control Components Release 20.14.1

Resolved Bugs for Cisco Catalyst SD-WAN Control Components Release 20.14.1

Identifier	Headline
CSCwi71976	UI changed needed for CSCwi56821 MT License Settings exposed at Tenant level.
CSCwi85554	Cisco SD-WAN Manager cannot deploy a configuration group on a cedge added by a tag rule
CSCwi45824	User with only Read permission for Cisco Edge devices can see controller devices Certificates.
CSCwh91838	The marking maintenance security deprecated.
CSCwi54372	Cisco SD-WAN Manager cloud onramp for Multicloud - cloud connectivity , audit is failing.
CSCwj12763	The IP name-server command not pushed to Cisco IOS XE Catalyst SD-WAN device.
CSCwi74398	DCA Rest: MT: If some tenant uploads fail, further tennats may be skipped.
CSCwh97427	RADIUS user with username format domain\xxxx get's logged out without minutes of logging in.
CSCwi28960	Cisco SD-WAN Validator crash with error "Software initiated - Daemon 'vbond_0' failed"
CSCwc04678	The data-policy-commit-failure notification promote to Alarm.
CSCwi92850	Export in Monitor Tunnels does not generate a file with the filter created.
CSCwj23827	Cisco SD-WAN Manager DR : Replication stuck and not even attempting to create further exports.
CSCwi56821	MT License Settings exposed at Tenant level.
CSCwi62044	SD-AVC container mount point change in Cisco SD-WAN Manager results in lost custom apps post-upgrade.
CSCwi10675	Devices with pull mode stats collection stops working after upgrade to 20.13 latest.
CSCwi21892	After Upgrade from 20.8.1 to 20.9.3.2, no graph on license and device overview page.
CSCwi21322	Cisco Catalyst SD-WAN Manager Release 20.13.1: Azure SD-Routing CoR: Multicloud Monitoring dashboard is not showing Gateway/VNET/TAG/VPN
CSCwi31742	Changes in copied configuration group is updating original CG.

Identifier	Headline
CSCwi60266	Cisco IOS XE Catalyst SD-WAN device with enterprise certificates not forming control connections with controllers after upgrade.
CSCwi45974	Unable to save the TACACS Server configuration when using Configuration Groups.
CSCwj04353	DCA is not sending device list data for MT Tenants.
CSCwi23194	Policy Groups 2.0 - Groups of Interest - Creating application difficult to do.
CSCwi21976	Cisco SD-WAN Manager API: User with only Interface read-only access can see the connected user list.
CSCwi75078	The banner issue on Cisco IOS XE Catalyst SD-WAN device from feature template Cisco SD-WAN Manager 20.9.4.1
CSCwi49242	After upgrading Cisco SD-WAN Manager to 20.12.2, local/AAA users won't be able to login after 10-15 mns reboot
CSCwi21221	QuickConnect UI fail to import, export and Create New site-id. Pop-up is not shown.
CSCwh73082	Few or All OMP peers stay Down after Cisco SD-WAN Controller cores (vCPU) are upgraded from 2 to 8.
CSCwi56971	Cisco SD-WAN Manager 20.12.2 / Search tool of Select smart/virtual accounts to fetch/sync licenses is not working
CSCwi95474	6 + 6 DR cluster elects replication leader which has no config-db and fails to connect to neo4j
CSCwi05347	The config failed with "probe-path should be configured as branch.." message when enable o365 telemetry.
CSCwi45443	The vdaemon file is incomplete when generating a Cisco SD-WAN Manager admin-tech using GUI.
CSCwj04397	ST Cisco SD-WAN Manager getting license alarms incorrectly.
CSCwi14897	RBAC by VPN groups is blocked on UI (verification failed) - multiple issues.
CSCwj39594	The 6-Node cluster DR Replication not working in certain scenario.
CSCwi21272	Password fields are not masked in Add and Review Device configuration page.
CSCwi72111	/dataservice/device/action/install/devices/{deviceType} not working in apidocs page.
CSCwi26347	Delete all VNF service fail under Network Design.
CSCwi35518	ND push fail to ENCS device: Invalid usage - Remove vlan before using vlan-range
CSCwi91763	On -Prem SSM has reporting broken.
CSCwi20779	Solution: retry logic needed for delete tunnel group from Cisco SD-WAN Manager.

Identifier	Headline
CSCwi12234	Workflow library: 'Do not show again' option on introduction of workflows not honoured.
CSCwi51188	Cross Platform Navigator: enable to navigate to Cisco services hosted in the Cisco Networking Cloud.
CSCwh33133	MD5 authentication: console logs include deprecation warning.

Open Bugs for Cisco Catalyst SD-WAN Control Components Release 20.14.1

Identifier	Headline
CSCwj28483	Deployment of Cloud Gateway in network without Multi Region Fabric functionality.
CSCwi81830	Cisco SD-WAN Manager 20.12.3: unable to login to Cisco SD-WAN Manager after enabling proxy- AAAMgr auth req failed with exception.
CSCwj43428	Cisco SD-WAN Manager-20.13.1 shows "add DNS IPv4" instead of "IPv6 Address Field" under Service-Profile SVI
CSCwj39215	Selecting 3-dots next to BGP feature does not save Edge01 or Edge02.
CSCwi01358	aaaMgr namespace is not created in one of the Cisco SD-WAN Manager after configuring radius server.
CSCwj44137	[20.14.0-201] ST-SIT: DR options not editable in Cisco SD-WAN Manager
CSCwj27809	500 Server Error: Internal Server Error for url: https://10.236.8.119/dataservice/statistics/system/
CSCwj44188	20.14 Zscaler SSE GRE MT: Error 429 from Zscaler API for activate is seen
CSCwj38614	Cisco SD-WAN Manager 20.13: Enforce Software Version (ZTP) selected version is not reflected after save
CSCwj53308	The sdwan controller not establish NTP over vpn 512 IPV6

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.

Cisco Catalyst SD-WAN Manager API

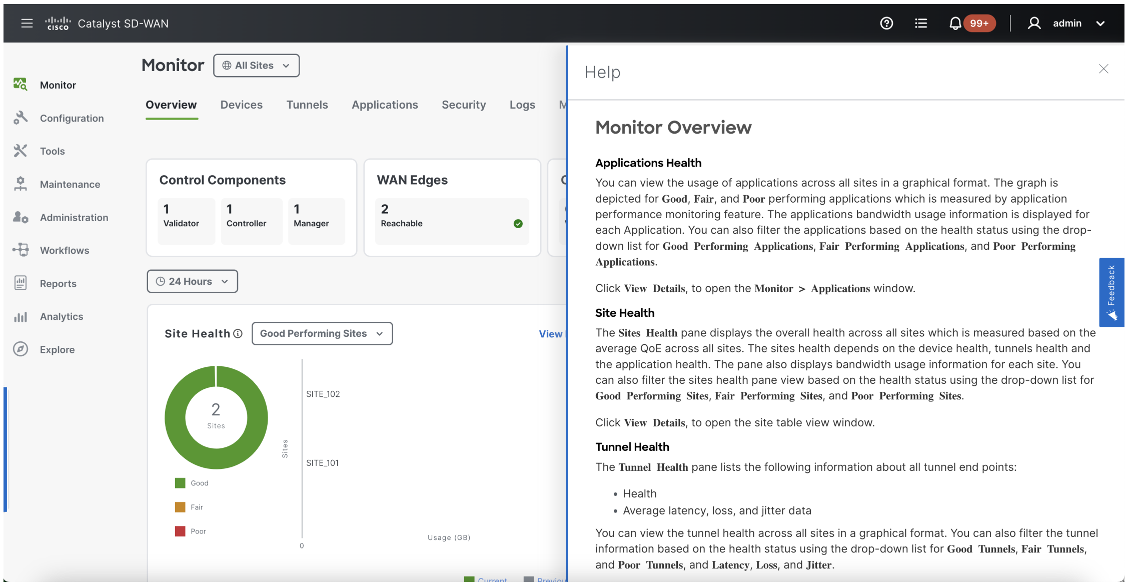
For information on Cisco SD-WAN Manager Release 20.14.x APIs, see Cisco SD-WAN Manager API.

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 1: Help Content in a Slide-in Pane



Monitor Overview

Applications Health

You can view the usage of applications across all sites in a graphical format. The graph is depicted for **Good**, **Fair**, and **Poor** performing applications which is measured by application performance monitoring feature. The applications bandwidth usage information is displayed for each Application. You can also filter the applications based on the health status using the drop-down list for **Good Performing Applications**, **Fair Performing Applications**, and **Poor Performing Applications**.

Click **View Details**, to open the **Monitor > Applications** window.

Site Health

The **Sites Health** pane displays the overall health across all sites which is measured based on the average QoE across all sites. The sites health depends on the device health, tunnels health and the application health. The pane also displays bandwidth usage information for each site. You can also filter the sites health pane view based on the health status using the drop-down list for **Good Performing Sites**, **Fair Performing Sites**, and **Poor Performing Sites**.

Click **View Details**, to open the site table view window.

Tunnel Health

The **Tunnel Health** pane lists the following information about all tunnel end points:

- Health
- Average latency, loss, and jitter data

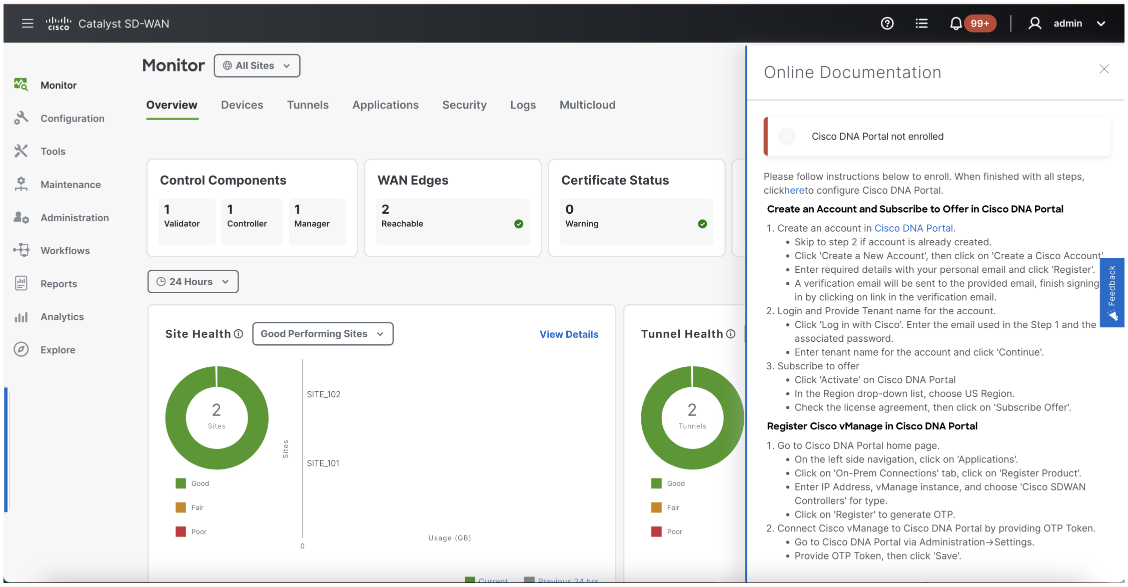
You can view the tunnel health across all sites in a graphical format. You can also filter the tunnel information based on the health status using the drop-down list for **Good Tunnels**, **Fair Tunnels**, and **Poor Tunnels**, and **Latency**, **Loss**, and **Jitter**.

Cisco DNA Sense

Access help content for Cisco SD-WAN Manager UI pages using Cisco DNA Sense by clicking the **?** icon at the top-right corner and choose **Online Documentation** from the drop-down list.

Cisco DNA Sense is not enabled by default for all the users. You should enroll and configure your Cisco SD-WAN Manager using the instructions provided in the **Online Documentation** pane. The help content from Cisco DNA Sense is displayed across all major Cisco SD-WAN Manager pages once you enroll.

If your Cisco SD-WAN Manager is already enrolled to Cisco DNA Sense, choose **Online Documentation** from the **?** drop-down.



Online Documentation

Cisco DNA Portal not enrolled

Please follow instructions below to enroll. When finished with all steps, clickhereto configure Cisco DNA Portal.

Create an Account and Subscribe to Offer in Cisco DNA Portal

1. Create an account in Cisco DNA Portal.
   - Skip to step 2 if account is already created.
   - Click 'Create a New Account', then click on 'Create a Cisco Account'.
   - Enter required details with your personal email and click 'Register'.
   - A verification email will be sent to the provided email, finish signing in by clicking on link in the verification email.
2. Login and Provide Tenant name for the account.
   - Click 'Log in with Cisco'. Enter the email used in the Step 1 and the associated password.
   - Enter tenant name for the account and click 'Continue'.
3. Subscribe to offer
   - Click 'Activate' on Cisco DNA Portal
   - In the Region drop-down list, choose US Region.
   - Check the license agreement, then click on 'Subscribe Offer'.

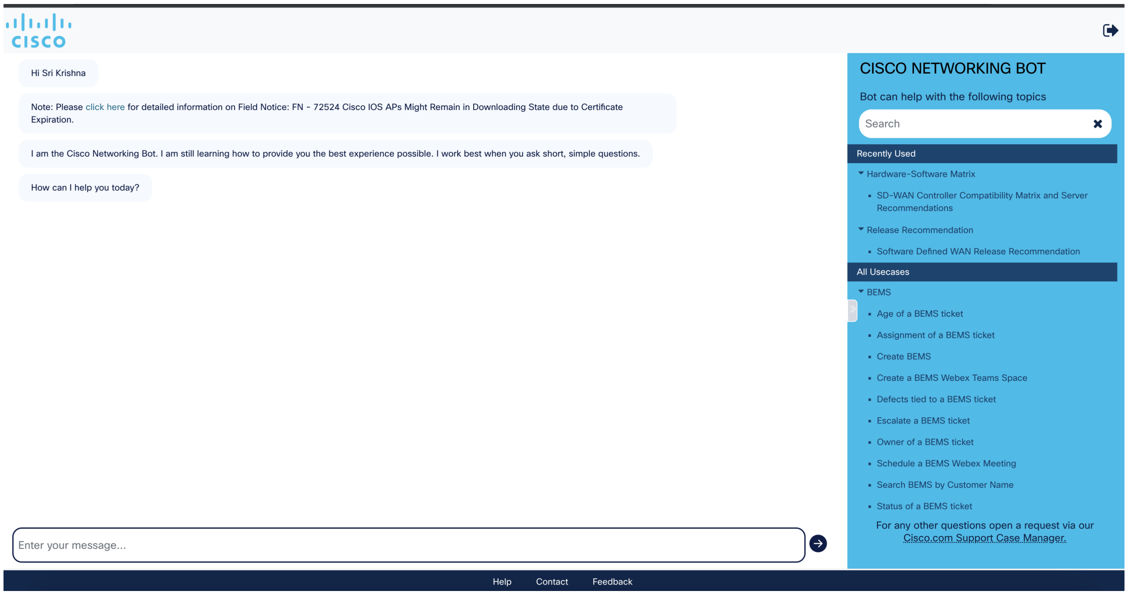
Register Cisco vManage in Cisco DNA Portal

1. Go to Cisco DNA Portal home page.
   - On the left side navigation, click on 'Applications'.
   - Click on 'On-Prem Connections' tab, click on 'Register Product'.
   - Enter IP Address, vManage instance, and choose 'Cisco SDWAN Controllers' for type.
   - Click on 'Register' to generate OTP.
2. Connect Cisco vManage to Cisco DNA Portal by providing OTP Token.
   - Go to Cisco DNA Portal via Administration→Settings.
   - Provide OTP Token, then click 'Save'.

Ask Cisco Networking Bot

To access the **Cisco Networking Bot** click the **Help(?)** icon and choose **Ask Cisco Networking** from the drop-down list.

You can use Cisco Networking Bot chat to get relevant answers to your questions.



Hi Sri Krishna

Note: Please click here for detailed information on Field Notice: FN - 72524 Cisco IOS APs Might Remain in Downloading State due to Certificate Expiration.

I am the Cisco Networking Bot. I am still learning how to provide you the best experience possible. I work best when you ask short, simple questions.

How can I help you today?

CISCO NETWORKING BOT

Bot can help with the following topics

Recently Used

- Hardware-Software Matrix
  - SD-WAN Controller Compatibility Matrix and Server Recommendations
- Release Recommendation
  - Software Defined WAN Release Recommendation

All Usecases

- BEMS
  - Age of a BEMS ticket
  - Assignment of a BEMS ticket
  - Create BEMS
  - Create a BEMS Webex Teams Space
  - Defects tied to a BEMS ticket
  - Escalate a BEMS ticket
  - Owner of a BEMS ticket
  - Schedule a BEMS Webex Meeting
  - Search BEMS by Customer Name
  - Status of a BEMS ticket

For any other questions open a request via our Cisco.com Support Case Manager.

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

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.

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.