Release Notes for Cisco vEdge Devices, Cisco SD-WAN Release 20.8.x

First Published: 2022-04-22

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 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 vEdge Device, Cisco SD-WAN Release 20.8.x



Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

These release notes accompany the Cisco SD-WAN Release 20.8.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 vEdge devices.

Related Releases

For release information about Cisco IOS XE Catalyst SD-WAN devices, refer to Release Notes for Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release 17.8.x.

For release information about Cisco SD-WAN Controllers, refer to Release Notes for Cisco SD-WAN Controllers, Cisco SD-WAN Release 20.8.x

What's New for Cisco SD-WAN Release 20.8.x

This section applies to Cisco vEdge 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 SD-WAN solution, see the *Resolved and Open Bugs* section in the Release Notes.

Table 1: Cisco SD-WAN Release 20.8.1

Feature	Description
Routing	
Verify OMP routes prefix	The verify keyword is added to "show omp route <prefix>" CLI to validate the availability of route on Cisco vEdge devices.
Policies	
Policy Checker on Cisco vSmart Controller	The test policy CLI enables you to troubleshoot large policies with numerous sequence numbers. This command identifies and displays the sequence number that matches a particular input variable and a policy name on Cisco vSmart Controllers.
Security	

Feature	Description
Layer 7 Health Check for Manual Tunnels	You can create and attach trackers to manually created GRE or IPSec tunnels to a SIG endpoint. Trackers help failover traffic when a SIG tunnel is down.
Single Sign-On Using Azure AD	Single Sign-On (SSO) with security assertion mark-up language (SAML) gives faster, easier, and trusted access to cloud applications without storing passwords or requiring you to log in to each application individually.
Cloud OnRamp	
Support for SVL Port Configuration on 100G Interfaces	With this feature, you can configure SVL ports on 100G Ethernet interfaces of Cisco Catalyst 9500-48Y4C switches, thus ensuring a high level of performance and throughput.
View Details of Microsoft Telemetry and View Application Server Information for Office 365 Traffic	This feature adds better visibility into how Cloud onRamp for SaaS determines the best path for Microsoft Office 365 traffic, if you have opted to use Microsoft telemetry. One enhancement is a chart that shows how Microsoft rates the connection quality of different interfaces, specifically for different types (called service areas) of Office 365 traffic. This is helpful for troubleshooting Office 365 performance issues. Another addition is the SD-AVC Cloud Connector page, which shows a list of Microsoft URL/IP endpoints and categories that Cisco SD-WAN receives from Microsoft Cloud.
User-Defined SaaS Application Lists	This feature expands the range of SaaS applications that Cloud onRamp for SaaS can monitor, and for which it can determine the best network path. The feature enables you to define lists of one or more SaaS applications, together with the relevant application server for those SaaS applications. Cloud onRamp for SaaS handles these lists in the same way that it handles the predefined set of SaaS applications that it can monitor. When you enable a user-defined list, Cloud onRamp for SaaS probes for the best path to the application server and routes the application traffic for applications in the list to use the best path.
Cisco SD-WAN Monitor and Maintain	
Software Upgrade Workflow for Cisco SD-WAN edge devices.	This feature introduces a guided workflow through which you can upgrade the software image on your Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices and monitor the status of the software upgrade. With this workflow, you can choose to download, install, and activate the new software image in discrete steps or in a single step.
Bidirectional Support for Packet Tracing	This feature provides a detailed understanding of how data packets are processed by the edge devices in both the directions. The bidirectional debugging can help you to diagnose issues and troubleshoot them more efficiently.
Cisco Hierarchical SD-WAN Configuration Guide	

Feature	Description
Hierarchical SD-WAN: Secondary Regions	Secondary regions provide another facet to the Hierarchical SD-WAN architecture and enable direct tunnel connections between edge routers in different primary access regions. When you assign an edge router a secondary region, the router effectively operates in two regions simultaneously, and has different paths available through its primary and secondary regions.
Hierarchical SD-WAN: Router Affinity	Often a router has multiple options to choose for the next hop when routing a flow to its destination. When multiple devices can serve as the next hop for a flow, you can specify the order of preference among the devices by configuring router affinity groups. The result is that a router attempts to use a route to the next-hop device of highest preference first, and if that device is not available, it attempts to use a route to the next-hop device of the next lower preference. Affinity groups enable this functionality without requiring complex control policies.

Software and Hardware Behavior Changes in Cisco SD-WAN Release 20.8.1

Behavior Change	Description
Support is no longer available for configuring an SNMPv3 user with the Secure Hash Algorithm (SHA-1) authentication protocol. You need to configure an SNMPv3 user with the SHA-256 authentication protocol.	A note is added in the Configure SNMPv3 on Cisco v
A new command **show support omp peer** is added to validate the availability of Cisco Catalyst SD-WAN Overlay Management Protocol (OMP) routes on Cisco vEdge devices.	A new command show support omp peer is added. A note is added in the Verify OMP Peer Sessions sec
Support is added for capturing IPv6 packets for tracing and troubleshooting. You can now choose an IPv6 interface from the **Interface** drop-down list.	A note is added in the Capture Packets section.
The **Application Usage** column and the **Application Usage** links are removed from the **Monitor** > **Devices** > **WAN - Tunnel** window. After configuring on-demand troubleshooting for a device, you can view SD-WAN Application Intelligence Engine (SAIE) usage data based on the selected filters or based on application families sorted by usage.	A note is added in the View TLOC Loss, Latency, ar A note is added in the View Tunnel Connections sec
Secure Internet Gateway (SIG) tracker monitor statistics are no longer reset at every Domain Name System (DNS) cache timeout interval. SIG tracker monitor statistics are now reset every two hours. A SIG tracker allows you to track the health of your SIG tunnels.	A note is added in the Create Automatic Tunnels Us
Alarms are added to syslog with syslog facility and priority `local7.notice`. A new command **show alarms history** is added for viewing the list of alarms raised in the past.	A new command show alarms history is added. Updated text is added in the Syslog Message Format

Behavior Change	Description
A new operational command **request nms server-proxy set management-ip** is added for entering the management IP address and port.	A new command request nms server-proxy is ad
Change in time-out behavior for template push to CCM.	In Cisco vManage Release 20.7.x and earlier rele device configuration tasks time out 30 minutes a long-running image installation operations, these the cluster activation state continues to be in a pe From Cisco vManage Release 20.8.1, the CCM a minutes after the last heartbeat status message that With this change, long-running image installatio fail after a predefined interval of time after task c
Change in CCM workflow.	In Cisco vManage Release 20.7.x and earlier rele activation progress is reported as part of the CLC seven steps in the CCM bring up and activation se successfully completed or not. The Push Feature of the RBAC settings configuration push. From Cisco vManage Release 20.8.1, CLOUD C vManage receives CCM Healthy from the target Configuration task shows the seven steps in the C indicates whether the sequence was successfully RBAC settings configuration push.

Important Notes, Known Behavior, and Workaround

- Starting from Cisco SD-WAN Release 20.5.1, Cloud onRamp for IaaS isn't supported for Cisco vEdge Cloud Router running on Cisco SD-WAN Release 20.5.1. However, Cloud onRamp for IaaS is supported with AWS as the cloud provider for Cisco vEdge Cloud Routers using Cisco SD-WAN Release 20.4.1 and earlier. Cloud onRamp for IaaS is also supported with Microsoft Azure as the cloud provider for Cisco vEdge Routers using Cisco SD-WAN Release 20.3.1 and earlier.
- For information about upgrade paths, see Cisco vManage Upgrade Paths.

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 SD-WAN Release 20.8.1

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 SD-WAN Release 20.8.1

Identifier	Headline
CSCwa92331	Affinity logic not working if entire CG1 vSmart shutdown
CSCwa67563	Cisco vEdge USB directory requires root access on 20.6
CSCwa82541	Cisco vEdge: ECMP for DP based DIA is not maintained if AAR policy applied

Open Bugs for Cisco SD-WAN Release 20.8.1

Identifier	Headline
CSCwb55566	FCV1: chassis-uuid missing in show output when Cisco vEdge-20.8.0.07-15 deployed w/ bootstrap-config
CSCwb52613	Cisco vEdge speed test will fail if the device system-ips has the same last 2 octets
CSCwd85121	After the vpn list change, the DP, AAR and CLFOWD polices stopped working on the routers.

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 SD-WAN Device Compatibility.

Cisco vManage GUI Changes

This section presents a comparative summary of the significant changes between Cisco vManage 20.7.x and earlier releases, and Cisco vManage Release 20.8.1.

Change in Control Labels

In Cisco vManage Release 20.8.1, the labels of the following UI elements have changed:

- **DPI** to **SAIE**: The deep packet inspection (DPI) flow is now called the SD-WAN Application Intelligence Engine (SAIE) flow. As a result, all UI elements related to DPI have been renamed as SAIE.

Figure 1: Example of Labels with DPI in Cisco vManage 20.7.x and Earlier Releases

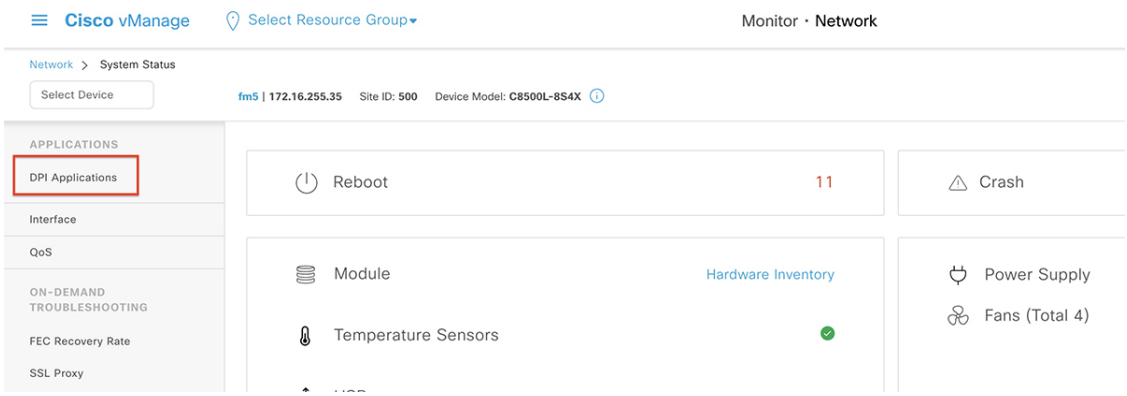
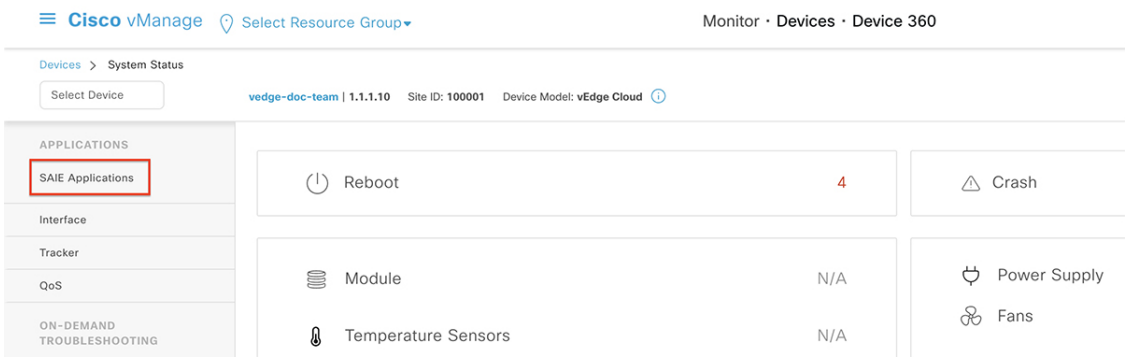


Figure 2: Example of Labels with SAIE in Cisco vManage Release 20.8.1



- **Device** to **Device Templates** (**Configuration** > **Templates**)

Figure 3: Device Tab in Cisco vManage 20.7.x and Earlier Releases

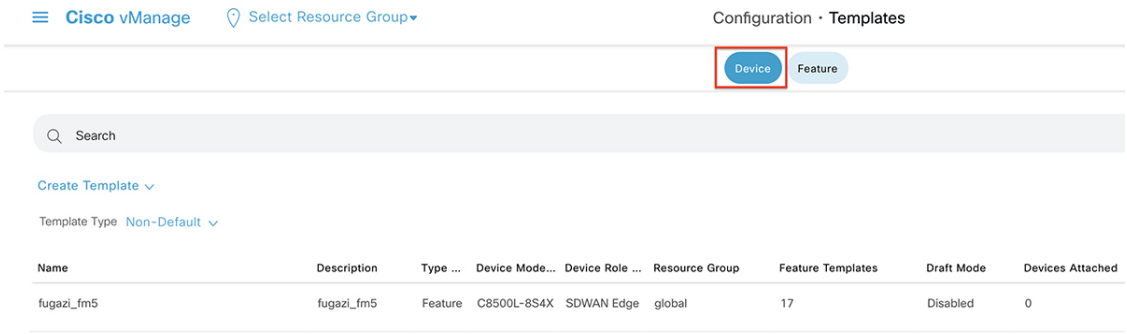
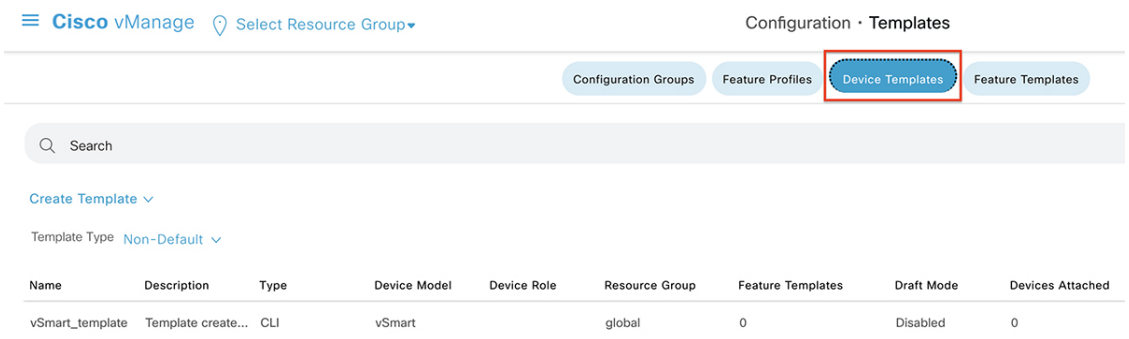


Figure 4: Device Templates Tab in Cisco vManage Release 20.8.1



- **Feature** to **Feature Templates** (**Configuration** > **Templates**)

Figure 5: Feature Tab in Cisco vManage 20.7.x and Earlier Releases

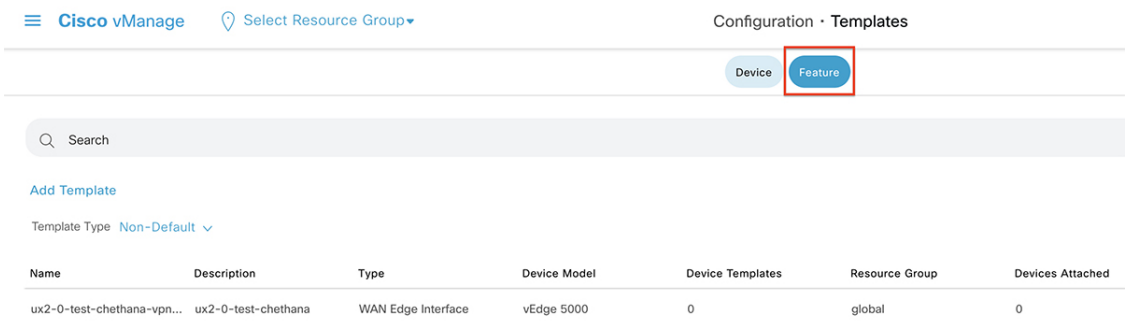
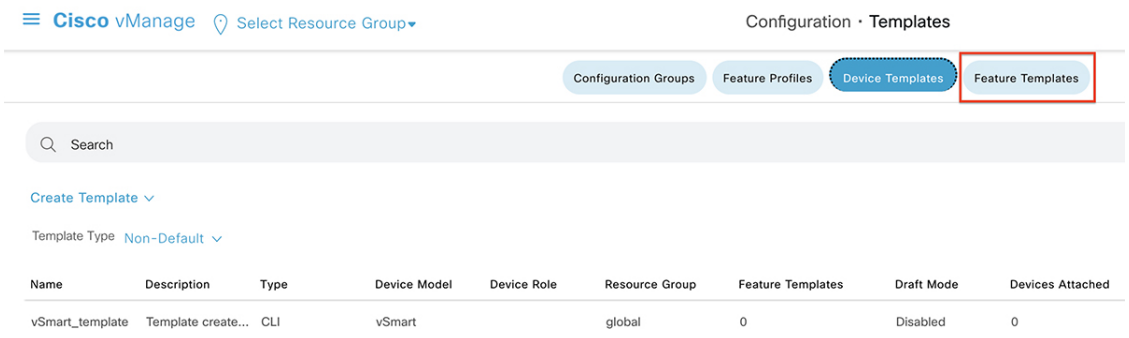


Figure 6: Feature Templates Tab in Cisco vManage Release 20.8.1



Support for Web Content Accessibility Guidelines (WCAG) 2.1 Standard

Cisco vManage Release 20.8.1 supports Web Content Accessibility Guidelines (WCAG) 2.1 standard for the AA conformance level, with the following limitations:

Table 2:

WCAG Success Criterion	Support	Limitation
2.1.2: No Keyborad Trap	Not Supported	You cannot exit from SSH terminal using the keyboard.

WCAG Success Criterion	Support	Limitation
2.4.5: Multiple Ways	Not Supported	You can locate pages on Cisco SD-WAN Manager using only one method.
1.1.1: Non-text Content	Partially Supported	Cisco SD-WAN Manager partially supports alternative text.
1.3.1, 3.3.1, 3.3.2, and 4.1.3: Screen Reader	Partially Supported	Cisco SD-WAN Manager partially supports screen reader for annoucements, error messages and data tables.
1.3.5: Identify Input Purpose	Partially Supported	Some input fields which collect personal information are not entirely supported by identify input purpose.
1.4.1: Use of color	Partially Supported	Cisco SD-WAN Manager uses colors to convey certain information and is partially compliant with WCAG 2.1 criterion for the use of colors.
1.4.3: Contrast	Partially Supported	Cisco SD-WAN Manager contains GUI elements that are not visible in the OS high contrast setting. Some text does not fully comply with the WCAG 2.1 color contrast ratio standards.
1.4.4: Resize text	Partially Supported	Cisco SD-WAN Manager partially supports browser resize text functionality.
1.4.10: Content reflow	Partially Supported	Cisco SD-WAN Manager partially supports content reflow.
1.4.11: Non-text contrast	Partially Supported	Cisco SD-WAN Manager partially supports non-text contrast ratio of 3:1.
1.4.13: Content on hover or focus	Partially Supported	Cisco SD-WAN Manager partially supports content on hover or focus.
2.1.1: Keyboard	Partially Supported	Cisco SD-WAN Manager elements provide partial support to access the elements using the keyboard.
2.4.2: Page titled	Partially Supported	Cisco SD-WAN Manager does not have meaningful page titles.

WCAG Success Criterion	Support	Limitation
2.4.3: Focus order	Partially Supported	Some elements in Cisco vManage do not have a logical focus order.
2.4.4: Link purpose (in-context)	Partially Supported	Cisco SD-WAN Manager partially supports link purpose (in context).
2.4.6: Headings and labels	Partially Supported	Cisco SD-WAN Manager partially supports label in name.
2.4.7: Focus visible	Partially Supported	Cisco SD-WAN Manager partially supports visible focus indicator.
2.5.3: Label in name	Partially Supported	Cisco SD-WAN Manager contains some accessible names that do not match with their visible label.
4.1.1: Parsing	Partially Supported	Some GUI elements do not have a unique ID on a page.
4.1.2: Name, role, value	Partially Supported	Cisco SD-WAN Manager contains some elements that do not have corrected names and roles.

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)

© 2022 Cisco Systems, Inc. All rights reserved.