# Release Notes for Cisco vEdge Devices and Cisco Catalyst SD-WAN Control Components, Cisco SD-WAN Release 20.4.x and Cisco Catalyst SD-WAN Control Components Release 20.4.x

**First Published:** 2020-09-30

**Last Modified:** 2023-05-11

## Release Notes for Cisco vEdge Device, Cisco SD-WAN Release 20.4.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 20.4.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.

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 Bengaluru 17.4.x.

## What's New for Cisco SD-WAN Release 20.4.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 20.4.1***

| Feature | Description |
|---|---|
| **Cisco SD-WAN Getting Started** | |

| Feature | Description |
|---|---|
| Support for Managing Root CA Certificates in Cisco SD-WAN Manager | This feature enables you to add and manage root certificate authority (CA) certificates. |
| Support for Subject Alternative Name (SAN) | This feature enables you to configure subject altenative name (SAN) DNS Names or uniform resource identifiers (URIs). It enables multiple host names and URIs to use the same SSL certificate. |
| **Systems and Interfaces** | |
| Static Route Tracker for Service VPNs for Cisco vEdge Devices | This feature enables you to configure IPv4 static route endpoint tracking for service VPNs.<br>For static routes, endpoint tracking determines whether the configured endpoint is reachable before adding that route to the route table of the device. |
| Assign Static IP Address to PPP Interface | This feature enables you to assign a static IP address to a PPP interface and configure PPP interface echo requests. |
| VRRP Interface Tracking for Cisco vEdge Devices | This feature enables VRRP to set the edge as active or standby based on the WAN Interface or SIG tracker events and increase the TLOC preference value on a new VRRP active to ensure traffic symmetry, for Cisco vEdge devices. |
| Cisco SD-WAN Multitenancy | With Cisco SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco vManage. In a multitenant Cisco SD-WAN deployment, tenants share Cisco vManage instances, Cisco vBond Orchestrators and Cisco vSmart Controllers. Tenant data is logically isolated on these shared resources. |
| Configure a Cisco vEdge Device as an NTP Parent | This feature enables configuring a Cisco vEdge device as an NTP parent and to configure the device to support NTP in symmetric active mode. |
| Configure a Cellular Gateway | This feature provides templates for configuring a supported cellular gateway as an IP pass-through device.<br>This release supports the Cisco Cellular Gateway CG418-E. |
| Support for Password Policies using Cisco AAA | This feature allows you to create password policies for Cisco AAA. Password policies ensure that your users use strong passwords and can be customized based on your requirements. To configure password policies, push the `password-policy` commands to your device using Cisco SD-WAN Manager device CLI templates. For more information on the `password-policy` commands, see the `aaa` command reference page. |
| **Policies** | |

| Feature | Description |
|---|---|
| Policy Matching with ICMP Message | This feature provides support for a new match condition that you can use to specify a list of ICMP messages for centralized data policies, localized data policies, and Application-Aware Routing policies.<br><br>For information on matching ICMP messages in a centralized data policy, see Match Parameters - VPN List.<br><br>For information on matching ICMP messages in a localized data policy, see Match Parameters.<br><br>For information on matching ICMP messages in a Application-Aware Routing policy, see Structural Components of Policy Configuration for Application-Aware Routing. |
| Traffic Redirection to SIG Using Data Policy | With this feature, while creating a data policy, you can define an application list along with other match criteria and redirect the application traffic to a Secure Internet Gateway (SIG). |
| Per-class Application-Aware Routing | This feature enahances the capabilities of directing traffic to next-hop addresses based on the SLA definitions. These SLA definitions along with the policy to match and classify traffic types can be used to direct traffic over specific Cisco SD-WAN tunnels. The SLA definition comprises of values of loss, latency and jitter, which are measured using the BFD channel that exists between two TLOCs. |
| **Security** | |
| IPSEC/GRE Tunnel Routing and Load-Balancing Using ECMP | This feature allows you to use the SIG template to steer application traffic to Cisco Umbrella or a Third party SIG Provider. The application traffic is steered to a SIG based on a defined data policy and other match criteria.<br><br>This feature also allows you to configure weights for multiple GRE/IPSEC tunnels for distribution of traffic over multiple tunnels. Equal-cost multi-path (ECMP) routing and load balancing is supported on multiple GRE/IPSEC tunnels. |
| **Cloud OnRamp** | |
| Support for Cisco Cloud Services Platform,CSP-5456 (Cloud onRamp for Colocation) | Starting from this release, Cisco CSP-5456 is supported on the Cloud onRamp for Colocation solution. The CSP-5456 offers a higher capacity of 56 cores, which maximizes the placement of VNFs in service chains. |
| Support for Cisco Catalyst 8000V Devices (Cloud onRamp for Colocation) | Starting from this release, Cisco Catalyst 8000V devices are now supported as a validated VNF in the Cloud onRamp for Colocation solution. |
| Onboarding CSP Device with Day-0 Configuration Using USB Drive (Cloud onRamp for Colocation) | This feature enables you to onboard CSP devices by loading the Day-0 configuration file to a USB drive. Use this onboarding option when you can't access the Internet to reach the Plug-and-Play Connect server. |

| Feature | Description |
|---|---|
| **High Availability Configuration Guide** | |
| Disaster Recovery for a 6 Node Cisco vManage Cluster | This feature provides validated support for disaster recovery for a 6 node Cisco vManage cluster. |

## Important Notes, Known Behavior, and Workaround

- Starting from Cisco SD-WAN Release 20.4.1.1, Microsoft Azure environment support is limited to deployment of Cisco SD-WAN controllers (Cisco vBond orchestrator, Cisco vSmart controller, and Cisco vManage) and the Cisco vEdge Cloud Router is not supported in Microsoft Azure.
- 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 vAnalytics service directly through Cisco SD-WAN Manager. In this case, log in to vAnalytics using this URL: https://analytics.viptela.com. If you can't find your vAnalytics login credentials, open a case with Cisco TAC support.
- For Cisco SD-WAN Release 20.4.1, you must run the messaging server on all the active instances of the Cisco SD-WAN Manager cluster when deploying the Cisco SD-WAN Manager cluster. See the High Availability Configuration Guide for vEdge Routers for more information.

## Cisco SD-WAN Manager Upgrade Paths

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

| Starting Cisco SD-WAN Manager Version | Destination Version | | | |
|---|---|---|---|---|
| | 19.2.x | 20.1.x | 20.3.x | 20.4.x |
| 18.x/19.2.x | Direct Upgrade | Direct Upgrade | Check disk space*<br>• If the disk space is more than 2GB: Direct Upgrade<br>• If the disk space is less than 2GB: Step upgrade through 20.1<br>• If you are upgrading to 20.3.5, the available disk space should be at least 2.5 GB.<br><br>For cluster upgrade procedure**: **request nms configuration-db upgrade**<br><br>**Note** We recommend the data base size in the disk is less than or equal to 5GB. Use the `request nms configuration-db diagnostic` command to check the data base size. This is applicable only for upgrades of devices running Cisco SD-WAN Manager Release 20.1.1 and later. | Step upgrade through 20.3 |

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

*To check the free disk space using CLI,

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

**Cluster upgrade must be performed using CLI

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

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

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

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

# Resolved and Open Bugs

### About the Cisco Bug Search Tool

Use the Cisco Bug Search Tool to access open and resolved bugs for a release.

The tool allows you to search for a specific bug ID, or for all bugs specific to a product and a release.

You can filter the search results by last modified date, bug status (open, resolved), severity, rating, and support cases.

## Bugs for Cisco SD-WAN Controller Release 20.4.2.3

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 Controller Release 20.4.2.3

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

## Bugs for Cisco vManage Release 20.4.2.3

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 vManage Release 20.4.2.3

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

## Bugs for Cisco vManage Release 20.4.2.2

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 vManage Release 20.4.2.2

| Bug ID | Description |
|---|---|
| CSCwa54712 | Evaluation of Cisco SD-WAN for Log4j 2.x DoS vulnerability fixed in 2.17 |

## Bugs for Cisco vManage Release 20.4.2.1

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 vManage Release 20.4.2.1

| Bug ID | Description |
|---|---|
| CSCwa47745 | Evaluation of Cisco vManage for Log4j RCE (Log4Shell) vulnerability |

## Bugs for Cisco SD-WAN Release 20.4.2

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 20.4.2

| Bug ID | Description |
|---|---|
| CSCvw13663 | Vedge_cloud_19.2.921 - FP misprogramming |
| CSCvx00210 | vEdge 5k crashed with reason "Software initiated - FP core watchdog fail" |
| CSCvx61152 | vSmarts crashing due to OOM after upgrade to 20.4.1.1 |
| CSCvy10840 | Cisco vManage available entropy exhaustion on some setup |

### Open Bugs for Cisco SD-WAN Release 20.4.2

| Bug ID | Description |
|---|---|
| CSCvy57394 | vEdge Cloud / 20.3.3 / Crash on bfdmgr_sla_class_next |

## Bugs for Cisco SD-WAN Controller Release 20.4.1.2

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 Controller Release 20.4.1.2

| Bug ID | Description |
|---|---|
| CSCvw50857 | Frequent crashes/kernel panics on vEdge 100 models |
| CSCvx49472 | Policy Template push failure from Cisco vManage 20.4.1.1 to 17.2 |
| CSCvx52311 | Order of DNS entries fails with <bad-element>dns-server-list</bad-element> |
| CSCvx57151 | Update button stops working after adding DHCP option |
| CSCvx60393 | Directory ownership changed after reload/upgrade |
| CSCvx66814 | Container logs seen growing unbounded without log rotation |
| CSCvx80910 | Devices goes "Out-of-sync" and can't re-push template with security policy and fail with "bad-cli" |

## Bugs for Cisco SD-WAN Release 20.4.1

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 20.4.1

| Bug ID | Description |
|---|---|
| CSCvu41291 | vmanage admin account getting locked out randomly - breaking cluster operations etc |
| CSCvu56004 | Removing a data prefix list from one match condition removes it from all |
| CSCvu61781 | user accounts get randomly locked temporarily (for 15 mins) |
| CSCvu91485 | vmanage failed to generate switchport clis via switchport feature template |
| CSCvv05427 | Files are not being truncated to recover disk space |
| CSCvv33126 | vManage Cisco VPN template generated wrong config for cEdge NAT port forwarding |
| CSCvv40531 | Issue setting up secondary OU in vManage 20.1.12 |
| CSCvv41341 | Higher memory utilization on vmanage 20.1 |
| CSCvv44894 | Web traffic is not properly recognized by DPI |
| CSCvv45021 | PPP feature templates cannot modify IP MTU on Dialer interfacce |
| CSCvv54169 | 17.4 vManage to 17.3 cEdge NAT Port Forward template push failed |
| CSCvv54844 | ConfigDB not updating username/password |
| CSCvv60818 | 20.4 next vManage: Error thrown when push CLI 'dialer down-with-vInterface' under Dialer interface |
| CSCvv71563 | umbrella error while editing security policy attached to the device for offline devices. |
| CSCvv86465 | vManage: Template Push fails with Unable to send line feed after string |
| CSCvv89447 | Cisco SD-WAN vManage cluster kills session after idle-timeout expires even when traffic is present |
| CSCvv90381 | Vedge reversing the src and dst MAC instead of using its own src-mac. |
| CSCvv92084 | vedge 20.4R: controller connections go down after QoS configs applied |
| CSCvw05540 | Template push failed with "Tunnel Route-via Interface" config |
| CSCvw10638 | Symantec Automated cert installation shows wrong vManage GUI info in 20.4 for cluster(MT/ST) setups. |
| CSCvw20597 | Variables missing in vManage during template push. |
| CSCvw22190 | Cluster activation failed because of a space in resource pool field in cluster config |

| Bug ID | Description |
|---|---|
| CSCvw23294 | vedge-2k temp sensors failing intermittently |
| CSCvw28512 | Difference in ip address of interface and json causing the stats db and config db in waiting |
| CSCvw38077 | UI throwing "Failed to list cluster information:Unknown error" on cluster management page |
| CSCvw48466 | vManage showing negative CPU value |
| CSCvw56320 | on-prem vmanage ungraded to 20.3.2 from 19.2.3 rebooting in an interval of 10-15 min |
| CSCvw68861 | Change for configdb query planner to hint more effectively via $param instead of old-style {param} |
| CSCvw70138 | Old vAnalytics setting should not be migrated into CloudServices from GUI |
| CSCvi59726 | Cisco SD-WAN vManage SQL Injection Vulnerabilities |
| CSCvi69962 | Cisco SD-WAN Information Disclosure Vulnerability |
| CSCvk28609 | Cisco SD-WAN vManage SQL Injection Vulnerabilities |
| CSCvk28656 | Cisco SD-WAN vManage SQL Injection Vulnerabilities |
| CSCvk28667 | Cisco SD-WAN vManage SQL Injection Vulnerabilities |
| CSCvs11276 | Cisco SD-WAN vManage Information Disclosure Vulnerability |
| CSCvs99259 | Cisco SD-WAN vManage SQL Injection Vulnerabilities |
| CSCvv42576 | Cisco SD-WAN vManage Cypher Query Language Injection Vulnerability |
| CSCvw08529 | Cisco SD-WAN vManage Cypher Query Language Injection Vulnerability |

### Open Bugs for Cisco SD-WAN Release 20.4.1

| Bug ID | Description |
|---|---|
| CSCvo21728 | vEdge forming duplicate control-connections after increasing number of cores on vSmart |
| CSCvu42726 | Vedge devices' BIDNTVRFD remote error to a new primary DC |
| CSCvv76467 | Vedge-5000:Auto IP feature not working on vedge5k |
| CSCvv81189 | Service (service chain) is not advertised on Cloud OnRamp IaaS |
| CSCvv81254 | vManage: Device template attach failure after migrating to vManage Cluster setup |
| CSCvv95991 | SDWAN 20.4/17.4 - vEdge5000 - PPPoE/FTMD crash@ftm_config_vpn_pppoe_client |

| Bug ID | Description |
|---|---|
| CSCvv98608 | config preview failed with Exception in callback: BGP AS Number couldn't be retrieved in service VPN |
| CSCvw00102 | vManage doesn't allow updates to device template without providing optional parameters |
| CSCvw14883 | Incorrect mapping for device specific variables from interface shaping rate |
| CSCvw16238 | Incorrect tag for omp routes in Real Time view |
| CSCvw22159 | vEdge-5000 is unable to recognize SFP without reloading |
| CSCvw28568 | Tags are not displayed properly on the mapping page when switching between Azure and AWS |
| CSCvw31595 | SG attach fails with Placement Failed Error - VM BW not met even though there are no SC's attached |
| CSCvw32065 | vManage : AppQoE stats does not reflect right data (wrt to flows/bytes) after page refresh |
| CSCvw33060 | MTT UI:Wrong info displayed for connected vmanage under operational command |
| CSCvw34465 | cEdge Hostname mismatch in vManage GUI after CLI template update push |
| CSCvw41702 | vmanage dpi classification incorrect |
| CSCvw42635 | vedge vrrp stuck in init state with the sub-interface's second address |
| CSCvw45153 | vManage - cannot remove NAT statement and associated interface together |
| CSCvw46769 | CLI template push to vBond fails with "Device failed to process request. null" error |
| CSCvw47429 | IPS Signature update - username that's more than 32 characters will fail with 'Maximum length: 64' |
| CSCvw47885 | unexpected behavior for nat-tracker on vedge100M |
| CSCvw49402 | PPPoE config on Gig interface failed , vManage not handling ip mtu and mtu correctly |
| CSCvw49470 | 20.3 - Failed to get AMP api key from threat grid server for deviceId: C8300-2N2S-6T-FDO2330A00K |
| CSCvw50483 | Dashboard stopped showing graphs and data post upgrade from 19.2.3 to 20.3.2 |
| CSCvw50664 | vManage Optional OSPF Configuration Removed when Device Template Updated |
| CSCvw52973 | vManage UI is not coming up thread are stuck while updating factory default templates during startup |
| CSCvw54567 | unable to create or edit any template. |
| CSCvw57693 | Stale outbound connection after ipsec tunnel deletion |

| Bug ID | Description |
|---|---|
| CSCvw58305 | UC SDWAN: Not able to see policy profile in Custom options. |
| CSCvw62293 | vManage - Cannot change DNS variables in interface template |
| CSCvw62341 | vManage Dashboard - Alarm time zone is tagging with incorrect time zone |
| CSCvw63123 | vManage generates unacceptable configuration for LTE controller |
| CSCvw65294 | Cisco vManage fails to activate/deactivate attached policies |
| CSCvw68402 | Template push to cEdge fails when changing system-ip due to vsmart centralized policy |
| CSCvw72087 | Full GC (Allocation Failure) on Standalone Cisco vManage running 264 devices |
| CSCvw54263 | 17.4: Duplicate sla-class info in the alrams on Cisco vManage |
| CSCvw45408 | Azure Node:Device Upgrade task stuck when 1 vManage node goes for a reboot |
| CSCvw45446 | Azure 6 Node: Cluster goes into a bad state for ~10 mins when OOB Intf in shut on 3rd vManage |
| CSCvw76649 | vManage 6 Node CLuster on Azure takes 2 mins to login to vManage UI. |
| CSCvw76757 | stats db is being killed by the kernel with OOM when sending dpi data |
| CSCvw86250 | OMP crash seen on vedges if duplicate system IP is configured on devices across different tenants |
| CSCvx68246 | Changing Config-DB ID/Password from default to non-default on a cluster of more than 3 members |
| CSCvw50857 | Frequent crashes/kernel panics on vEdge 100 models |
| CSCvx49472 | Policy Template push failure from Cisco vManage 20.4.1.1 to 17.2 |
| CSCvx37901 | nms_bringup file has ^M in each line after service restart as part of DR |

## 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.

## 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)

© 2021 Cisco Systems, Inc. All rights reserved.