



Cisco Nexus Dashboard Insights Fabrics, Release 6.5.x - For Cisco ACI

Table of Contents

New and Changed Information	2
Fabrics	3
Fabrics	3
Prerequisites	3
Guidelines and Limitations	3
Add fabrics	4
Fabric Details	8
Working with Fabrics	11
Copyright	12

First Published: 2024-06-28

Americas Headquarters

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

<http://www.cisco.com>

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

New and Changed Information

The following table provides an overview of the significant changes up to the current release. The table does not provide an exhaustive list of all changes or the new features up to this release.

New Features and Changed Behavior in the Cisco Nexus Dashboard Insights

Feature	Description	Release	Where Documented
Terminology change	The term "sites" is renamed to "fabrics".	6.5.1	Entire document

This document is available from your Cisco Nexus Dashboard Insights GUI as well as online at www.cisco.com. For the latest version of this document, visit [Cisco Nexus Dashboard Insights Documentation](#).

Fabrics

Fabrics

Fabrics are on-premises network regions that consist of a group of switches and other networking devices that provide connectivity for your applications and endpoints. You can split fabrics into different availability zones, such as pods, that are analyzed and managed by Nexus Dashboard Insights.

Types of on-premises fabrics

- Online fabrics: Multiple Nexus switches running ACI or NX-OS that can be represented by a controller such as APIC or NDFC and connected to Nexus Dashboard Insights to continuously stream telemetry. Types of online fabrics include:
 - ACI: Multiple Nexus switches with Cisco ACI and represented by a Cisco APIC.
 - NDFC: Multiple Nexus switches with Cisco NX-OS and represented by a Cisco NDFC.
 - NX-OS: A group of Cisco Nexus 9000 switches running NX-OS without a controller.
- Snapshot fabrics: Controller-based fabrics, that are referenced by a snapshot, for use in one-time analysis or demonstrations. They may or may not be connected to Nexus Dashboard Insights over the network.

To learn about how to prepare fabrics for onboarding, see [Add fabrics](#).

Once your fabric is onboarded and fully prepared, Nexus Dashboard Insights will start the fabric analysis to collect data from your fabric and display the fabric information in the **Fabrics** page. See [Fabric Details](#). From there, you can view your fabric's general information, inventory, L2 and L3 connectivity, endpoints, anomalies and advisories and more! To learn more see [Fabric Details](#).

Prerequisites

- You have configured DNS on the fabric. See [Configure DNS](#).
- You have configured NTP on the fabric. See [Configure NTP in ACI Fabric Solution](#).
- You have configured in-band management network. See [Cisco APIC and Static Management Access](#)
- You have configured out-of-band management on the controllers and switches.
- You have configured Fabric connectivity in Cisco Nexus Dashboard's Admin Console. See [Cisco Nexus Dashboard Platform Overview](#).
- You have the supported software version for your fabric. See [Nexus Dashboard and Services Compatibility Matrix](#).
- For snapshot fabrics, you have Python3 installed on your system.

Guidelines and Limitations

When you onboard a Cisco ACI fabric using the **Ready to Add** option in Nexus Dashboard Insights,

you cannot specify the **Login Domain** in Nexus Dashboard Insights. You can specify the **Login Domain** in Nexus Dashboard's Admin Console.

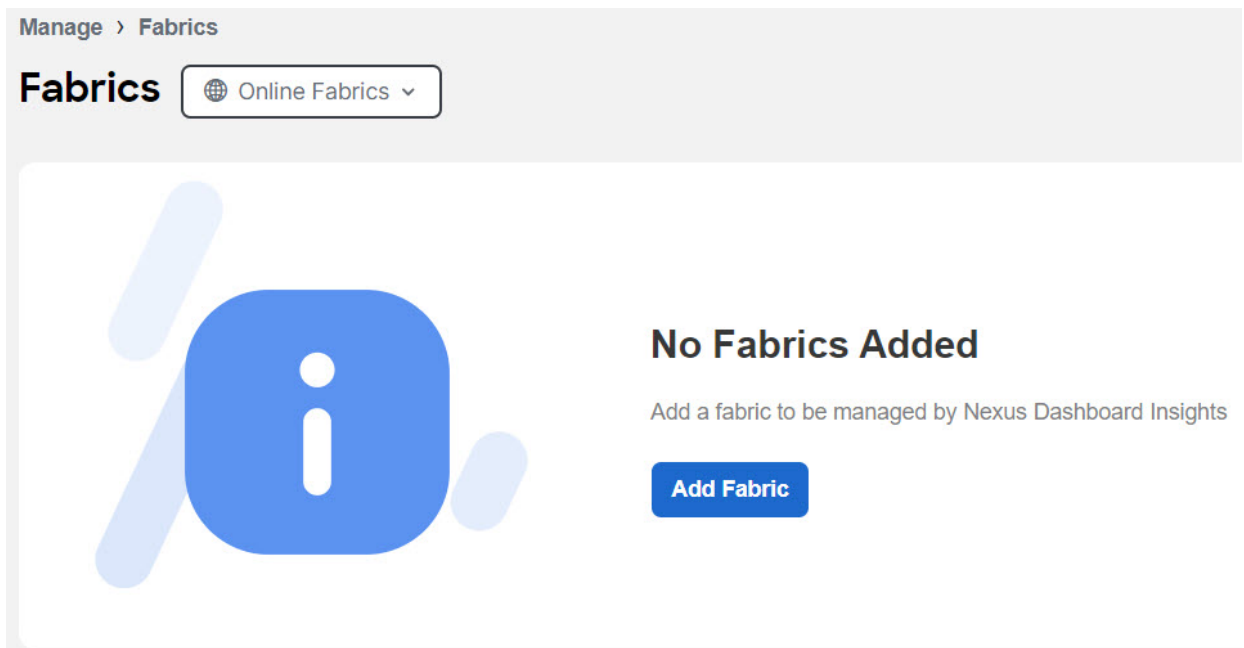
Add fabrics

You can add a fabric to Nexus Dashboard Insights using the following methods:

- Online fabrics
 - Enable the fabric that has already been added to Nexus Dashboard. Fabrics added to the Nexus Dashboard are not enabled in the services by default, so you will need to explicitly enable them directly from Nexus Dashboard Insights.
 - Add a fabric directly to Nexus Dashboard Insights.
- Snapshot fabrics
 - Add a snapshot fabric.

Add an online fabric

1. Navigate to **Manage > Fabrics**.
2. Click **Add Fabric**.
 - a. If you are adding a fabric in Nexus Dashboard Insights for the very first time, you will receive the following message. Click **Add Fabric** to proceed.



3. To enable a fabric that has been already added to Nexus Dashboard, choose **Ready to Add**. The fabrics added to Nexus Dashboard are displayed. To add a fabric to Nexus Dashboard, see [Cisco Nexus Dashboard Fabrics Management](#).

Add Fabric to Insights

You can add an ACI or NDFC controller to be part of a fabric.

[What is a Fabric?](#) | [How to prepare your ACI and NX-OS Fabric for Insights?](#)

1 Add Fabric

2 Details

3 Configuration

4 Summary

Ready To Add

Manually Add

Add Fabric Snapshot

Ready To Add

We found 2 fabrics that are already added to Nexus Dashboard but have not yet enabled Insights.

	Name	Type
☐	 candid6-AddFailTest	ACI
☐	 NS2	NDFC

<

Cancel

Back

Next

4. Complete the following fields for **Ready to Add**.

- Choose the fabric.
- Click **Next**.
- Click **See on map** and click the fabric location on the map to identify the fabric in the Admin Console.
- Click **Next**.
- For **Insights Collector Configuration**, use the toggle to choose IPv4 or IPv6 to onboard the fabric. Based on this setting, Nexus Dashboard Insights will configure its collector to receive telemetry from this fabric. This setting should match your fabrics IP address configuration.



IPv6 is only supported for Cisco APIC release 6.0(3) and later.

- In the **EPG** drop-down list, choose the in-band EPG. For Nexus Dashboard Insights, the in-band EPG is used for connectivity between Nexus Dashboard and the fabric.
- Click **Next**.
- Verify the configuration.
- Click **Save**.

5. To add a fabric to Nexus Dashboard and then enable the fabric using Nexus Dashboard Insights, choose **Manually Add**.

Add Fabric to Insights

You can add an ACI or NDFC controller to be part of a fabric.

[What is a Fabric?](#) | [How to prepare your ACI and NX-OS Fabric for Insights?](#)

6. Complete the following fields for **Manually Add**.

- In the **Hostname** field, enter the IP address used to communicate with the fabric's controller.
- In the **User Name** and **Password** field, provide the login credentials for a user with **admin** privileges on the fabric you are adding.
- In the **Domain** field, enter the controller login domain name.
- Click **Next**.
- Enter the fabric name to identify the fabric on Nexus Dashboard.
- Choose the fabric location from the map to identify the fabric on Nexus Dashboard.
- Click **Next**.
- Choose the in-band EPG from the drop-down list. For Nexus Dashboard Insights, in-band EPG is used for connectivity between Nexus Dashboard and the fabric.
- For **Insights Collector Configuration**, use the toggle to choose IPv4 or IPv6 to onboard the fabric. Based on this setting, Nexus Dashboard Insights will configure its collector to receive telemetry from this fabric. This setting should match your fabrics IP address configuration.



IPv6 is only supported for Cisco APIC release 6.0(3) and later.

- Enter the username and password. Enter the username with this format:

apic#<domain>\\<username>

Example: **apic#MyDomain.com\\MyUsername**

- Click **Next**.
- Verify the configuration.
- Click **Submit**.

Add a snapshot fabric

1. Navigate to **Manage > Fabrics**.
2. Click **Add Fabric**.
3. To add a snapshot fabric, choose **Add Fabric Snapshot**.

4. Click **Download Snapshot Script** to download the **data-collectors.tar.gz** to your machine.
5. Extract the file you downloaded and run the data collection script. Follow the instructions provided in the readme.md file. After the script is completed successfully, the data is collected in a **<filename>.tar.gz** file.



The collection script requires that you have Python3 installed on your system.

6. Upload the file in Nexus Dashboard Insights and click **Next**
7. Enter the fabric name to identify the fabric on Nexus Dashboard.
8. Choose the fabric location from the map to identify the fabric on Nexus Dashboard.
9. Click **Next**.
10. Verify the configuration.
11. Click **Submit**.

After your fabric is onboarded and fully prepared, Nexus Dashboard Insights will start the analysis to collect data from your fabric and display the fabric information in the **Fabrics** page. See [Fabric Details](#). The Fabric Analysis banner displays the progress of the analysis. The time to run the analysis depends on the size of the fabric.

Fabric Analysis - In Progress

Data collection is being performed on Site kw-ncaci101 to run corresponding analysis. [View System Status](#)

Fabric Details

In Nexus Dashboard Insights, **Global View** provides bird's eye view of your global network infrastructure for all your fabrics. The Fabrics page provides the details for an individual fabric.

For multi-cluster deployments see section Multi-Cluster Connectivity in [Journey and Global View](#).

Fabric Details in Global View

After you add the first fabric, **Global View** gives you a bird's eye view of your global network infrastructure for all your fabrics, their locations, and the key health metrics.

Navigate to **Overview > Global View**.

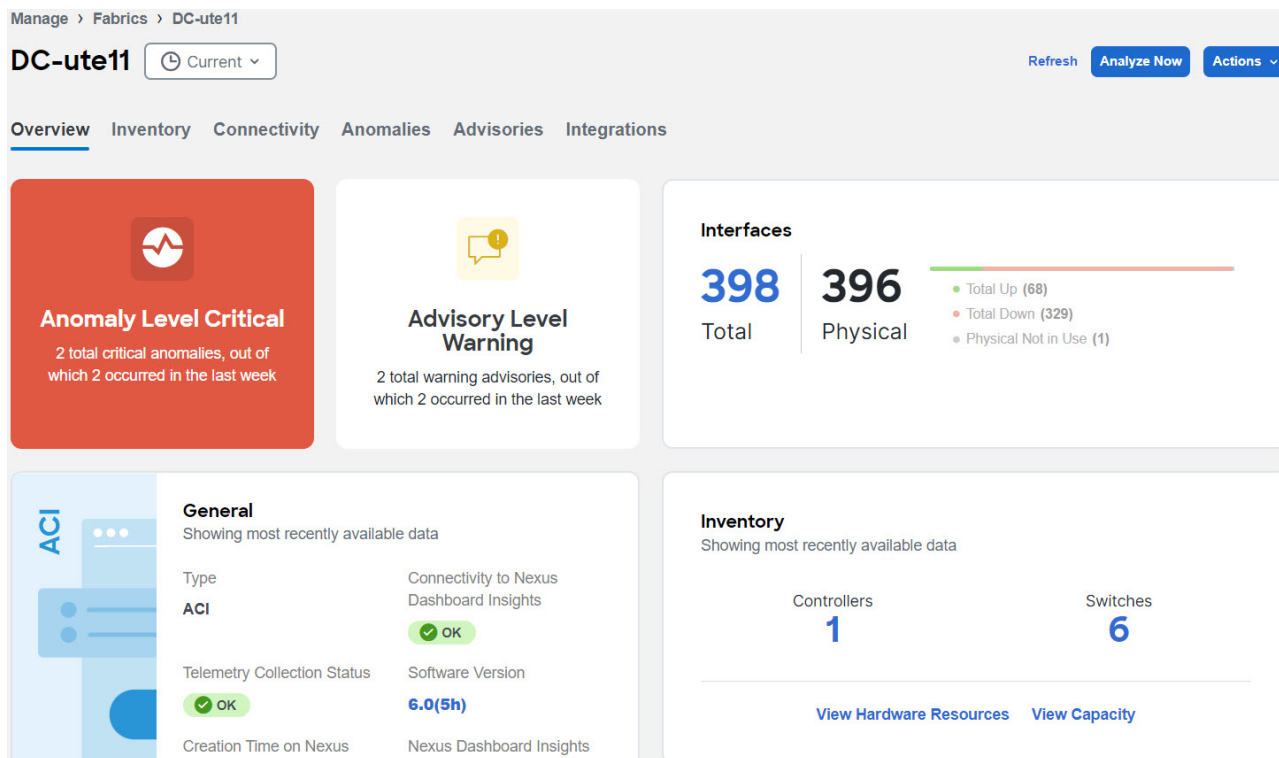
The map visually shows the physical location and total number of your fabrics in each continent, and their names. Click a fabric to jump directly to the details for that fabric, or scroll down to the Fabrics area to navigate to your fabric. You can also use the zoom control icons in the page to change your view of the map.

See an at-a-glance summary for each individual fabric in the Fabrics area. It includes their anomaly and advisory health levels, fabric-external traffic with total data transferred, and connectivity data for endpoints and Layer 3 neighbors. To learn about fabrics in Global View, see [Journey and Global View](#).

Individual Fabric Details

In the Fabrics page, you can dive into the details for an individual fabric, switch, or interface, with a comprehensive dashboard, simple topology, per-device summaries and more. You can also manage anomalies and advisories at a fabric level.

1. Navigate to **Manage > Fabrics**.
2. Choose Online or Snapshot fabrics from the drop-down list.
3. Use the search bar to filter the fabrics. The Fabrics table, displays the fabric type, connectivity status, anomaly and advisory level, onboarding time.
4. Click the fabric name to view details for your fabric.
5. From the Time Selection drop-down menu select the time. All sections will show data based on time selection and data availability. By default, the current time is selected.
6. Click **Overview**.



- a. In the **The Anomaly and Advisory** area you can view the status of your anomaly and advisory levels, and a list of your top anomaly and advisory categories.
 - i. Click **Anomaly** to view the level, category, and count for your anomalies for the fabric.
 - ii. Click the anomaly name to view additional details.
 - iii. Click **Advisory** to view the level, category, and count for your advisories for the fabric.
 - iv. Click the advisory name to view additional details.
- b. The **General** area shows you the type of fabric, the software version used, the connectivity status to Nexus Dashboard, conformance status, onboarding time, and telemetry status. In the General area hover on the software version and click **View Bugs** to view the active and susceptible bugs for that fabric. See [Getting Started](#). Telemetry collection status provides insights into the health and performance of the switches and devices in your network. The different telemetry collection statuses at the fabric level include:
 - i. **OK** - This status indicates that the telemetry data streaming from all the switches to Nexus Dashboard Insights is functioning correctly. This is the desired state, as it ensures comprehensive monitoring and visibility into the network's performance.
 - ii. **Not OK** - This status indicates the telemetry data streaming from all the switches to Nexus Dashboard Insights is not functioning correctly. This could be as a result of various problems such as network outages, misconfigurations, or hardware failures.
 - iii. **Partial OK** - This status indicates that telemetry data streaming from all the switches to Nexus Dashboard Insights is not functioning correctly from some of the switches but it is functioning correctly from others. This suggests an inconsistent or partial telemetry data flow within the network which could be caused by various factors, such as switch-specific issues or misconfigurations on some switches.
- c. In the **Analytics Summary** area, you can see an overview of the multiple analytics collected from across the fabric. It displays the status for conformance, sustainability and traffic analytics.
- d. In the **External Traffic** area, you can see the External Traffic that the fabric has sent and

received in the last 7 days. The donut helps view the how much traffic is sent and received by the fabric. Click the information icon to view more information about what External Traffic is and how it can be measured for the different types of fabrics.

- e. In the **Interfaces** area, you can see the summary of the interfaces for the fabric. Click **Total** to view additional details such as Anomaly Level, Admin Status, Operational Status, and Interface Type. Click the interface name to view additional details.
- f. In the **Connectivity** area, you can view details about your endpoints, and L3 neighbors.
- g. In the **Inventory** area, you can view the summary of the controllers and switches for the fabric.
 - i. Click **View Hardware Resources** to view the hardware resources for the fabric. Click and choose a resource from the **Top Devices By** drop-down list to see a graph for that resource. In the table that follows, see the resource usage by switch. Click the switch name to view additional details.
 - ii. Click **View Capacity** to view the different resources with their maximum capacity and current usage. Fabric Summary shows you the trends for the week, as well as the capacity by resource for the entire fabric. You see the number of resources used out of the total available capacity for each resource in this fabric (for example, Bridge Domains 2829 of 15000). The percentage indicates the percentage of resource used. The Switch Summary displays the capacity breakout of resources by switch. The graph shows you the timeline for the parameter that you have chosen from the **Top Switches By** drop-down list. In the table, click Operational Resources, Configuration Resources, or Hardware Resources, to see the capacity and usage for each switch in the fabric.
7. Click **Inventory** to view the the controllers and switches information for the fabric. To learn more, see [Inventory](#).
8. Click **Connectivity** to view the details of interfaces, endpoints, L3 neighbors, vPC Domains, flows for the fabric. To learn more, see [Inventory](#).
9. Click **Anomalies** to view all the anomalies for the fabric. To learn more, see [Anomalies and Advisories](#).
10. Click **Advisories** to view all the advisories for the fabric. To learn more, see [Anomalies and Advisories](#).
11. Click **Integrations** to view all the integrations associated with the fabric. To learn more, see [Integrations](#).
12. Click **File History** to view he history of files that are attached to the snapshot fabric. It shows the file name, the file size, when the file was uploaded, upload status, and when the last analysis was run.

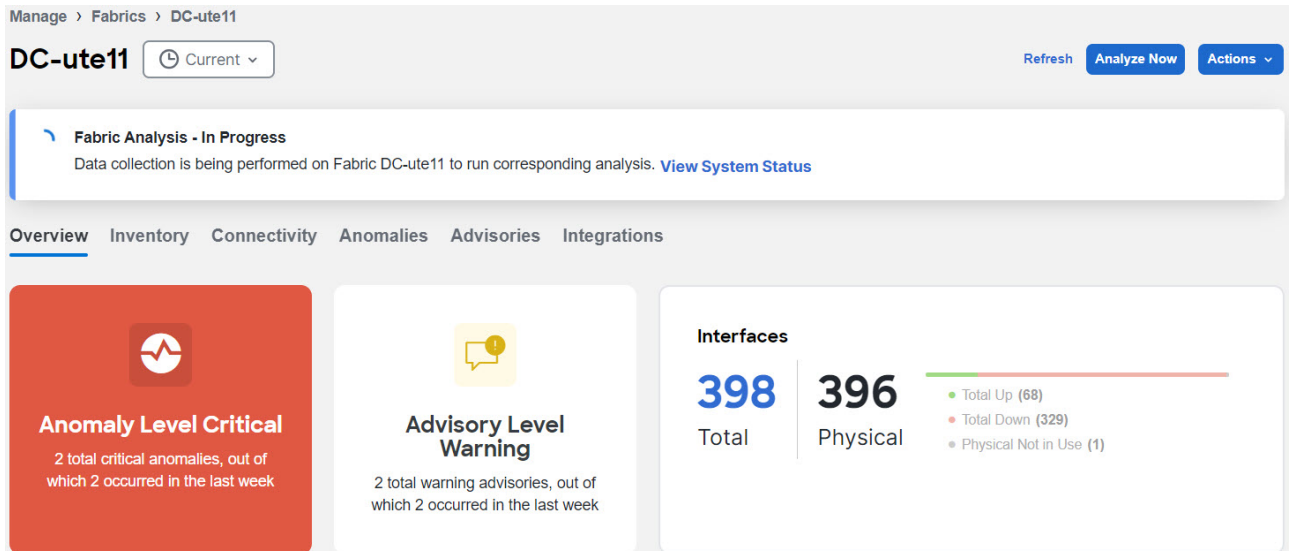


File History is displayed only for snapshot fabrics.

- a. For the currently active snapshot, which is the latest file that you uploaded, you can click **Run Analysis** to run the same snapshot analysis again. This can be useful when additional features are added and you want to re-run an analysis so that the additional features are included in your analysis.
- b. You can also upload a snapshot file for the same fabric at a different time interval. Click **Upload File** to upload the file and then click **Run Analysis** to run the snapshot analysis.

Working with Fabrics

1. Navigate to **Manage > Fabrics**.
2. To add a fabric, click **Add Fabric**. See [Add fabrics](#).
3. Choose Online or Snapshot fabrics from the drop-down list.
4. Click the fabric name to view the Fabric Details.



5. From the Actions drop-down menu, choose **Edit Fabric** to edit the fabric details. After you update the information, click **Save**.
6. From the Actions drop-down menu, choose **View in Topology** to view the topology for the fabric.
7. From the Actions drop-down menu, choose **System Status** to view the status of the data analysis for your fabric. See [Getting Started](#).
8. To delete a fabric from Nexus Dashboard Insights, perform the following steps:
 - a. From the Actions drop-down menu, choose **Pause Telemetry Collection** to pause data collection.
 - b. From the Actions drop-down menu, choose **Remove from Insights** to remove the fabric. The fabric is removed from Nexus Dashboard Insights only and not from Nexus Dashboard's Admin Console.
9. From the Actions drop-down menu, choose **Resume Telemetry Collection** to resume data collection.
10. Click **Analyze Now** to perform an on-demand analysis. Choose the service such as Assurance or Bug Scan and click **Run Now**. See [Getting Started](#).

Copyright

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.

The documentation set for this product strives to use bias-free language. For the 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 RFP documentation, or language that is used by a referenced third-party product.

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. (1110R)

© 2017–2025 Cisco Systems, Inc. All rights reserved.