Easy Deployment Guide for Cisco Secure Firewall 1000, 2100, and 3100 Series

First Published: 2020-10-28

Last Modified: 2022-07-20

Easy Deployment Guide for Secure Firewall Threat Defense 1000, 2100, and 3100 Series

This document provides information about two easy deployment options for Secure Firewall Threat Defense devices, low-touch provisioning for Cisco Defense Orchestrator (CDO) customers and low-touch provisioning for cloud-delivered Firewall Management Center customers.

This document is targeted for the following device models:

- Firepower 1000 series devices with software version 7.2 or later installed.
- Firepower 2100 series devices with software version 7.2 or later installed.
- Secure Firewall 3100 series devices with software version 7.2 or later installed.

Note The cloud-delivered Firewall Management Center supports current CDO users and devices configured for FDM. Devices must be running version 7.2 and later. For earlier versions, you can use CDO's device manager functionality. See the low-touch provisioning procedure in the Managing FDM Devices with CDO guide.

Branch Manager: Prepare and Connect a New Secure Firewall Threat Defense Device to Your Network

Low-touch provisioning allows anybody to connect a new Firepower 1000, Firepower 2100, or Secure Firewall 3100 series device to their network so that their IT department can onboard the device to CDO and configure it remotely.

Do you need to reimage your device?

If you device is not already running version 7.2, you can reimage the device and set it up for low-touch provisioning. This process does remove all existing policy configurations. To reimage your device to version 7.2, see the appropriate guide for your device model:

- Firepower 1010 series devices.
- Firepower 1100 series devices.
- Firepower 2100 series devices.

- Secure Firewall 3100 services devices.

Note that low-touch provisioning requires that the device has not been registered to, or previously associated with, a managing platform such as the Firepower Device Manager or a . If the device is currently registered to a manager, onboarding with low-touch provisioning fails.

Connect a New FTD to Your Network

As a branch manager, use the following procedures to correctly cable the device and connect to the network:

1. Before you rack the device or throw away the shipping carton, record your device's serial number and send it to your IT department. They need it to manage the device. The serial number of the device is located on the shipping carton the device came in, and on a label affixed to the device itself. See Find Your Device's Serial Number, on page 4 for more information.
2. Unpack the box and take inventory of the contents. Keep the shipping carton until you have plugged in the device, you have connected it to your network, and the device has successfully contacted the Cisco cloud.
3. Connect the device to power.
4. Connect the network cable from the Ethernet 1/1 interface to your WAN modem. Your WAN modem is your branch's connection to the internet and your firewall's route to the internet as well.

Note Do not connect the network cable from the device's Management interface to your WAN.

Figure 1: Firepower 1010 Cabling

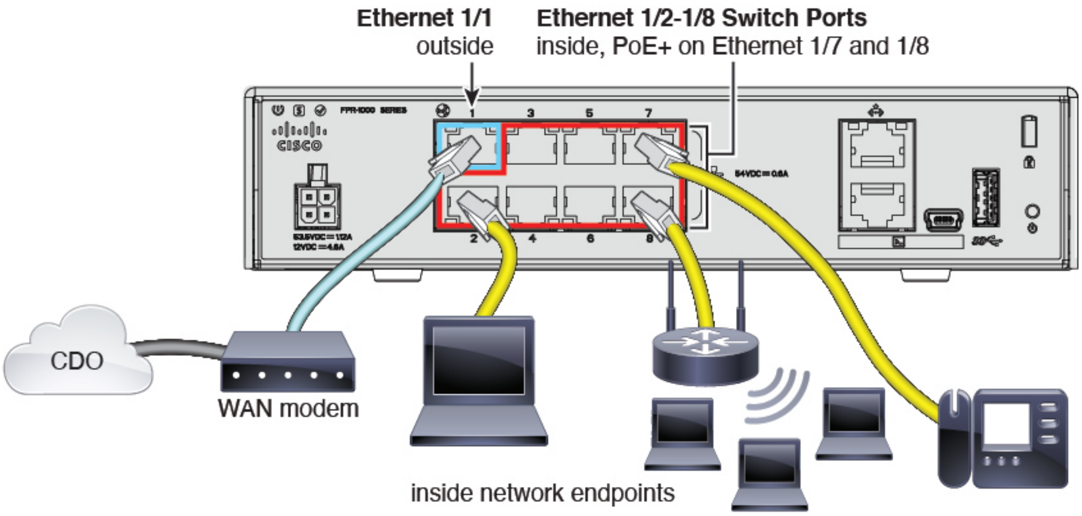

Ethernet 1/1
outside
Ethernet 1/2-1/8 Switch Ports
inside, PoE+ on Ethernet 1/7 and 1/8
CDO
WAN modem
inside network endpoints

Figure 2: Firepower 1100 Cabling

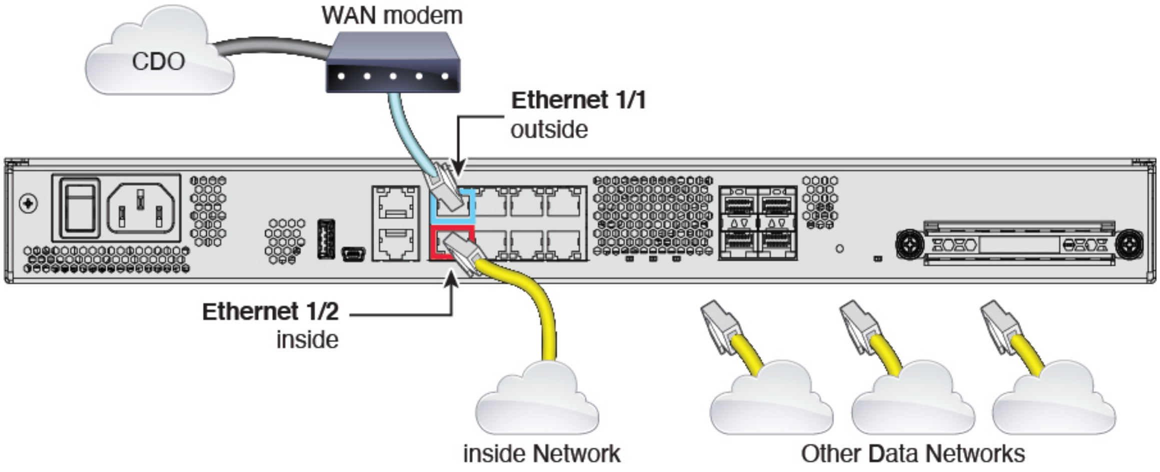


Figure 3: Firepower 2100 Cabling

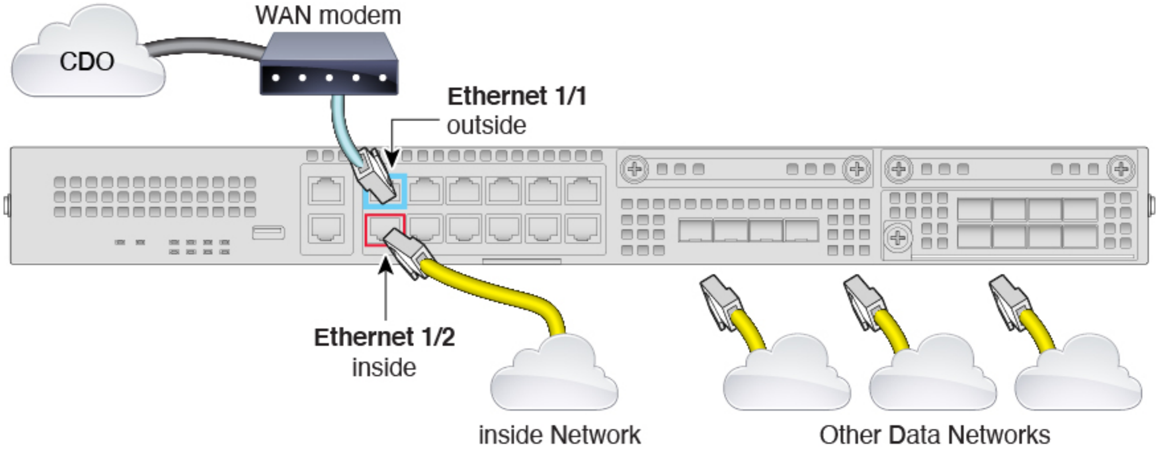
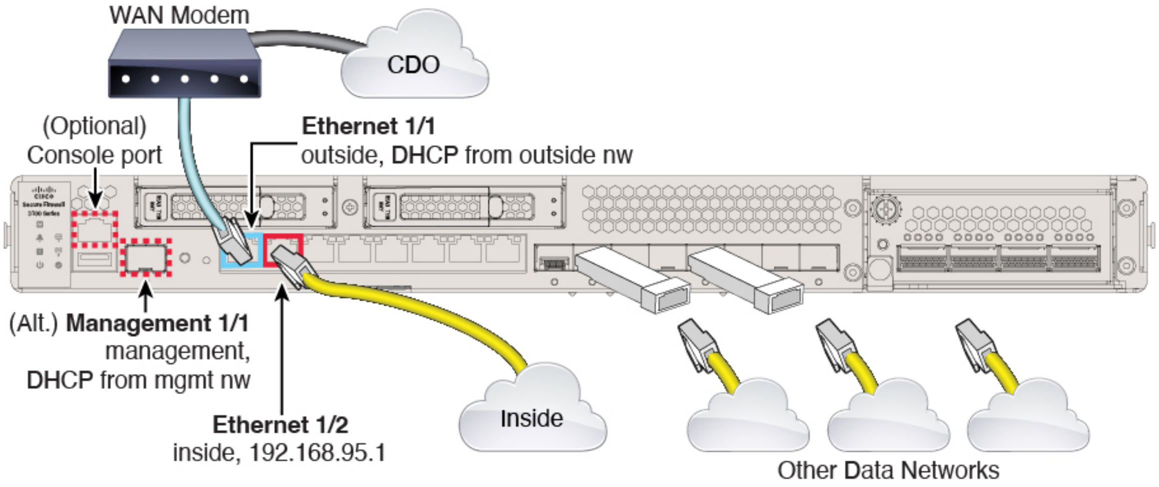


Figure 4: Secure Firewall 3100 Cabling



5. Observe the Status, SYS, or M LED on the device to determine if the device has reached the Cisco cloud. The table below provides the LED statuses and the approximate time they occur after the you connect the ethernet cables. It may take a little more time or a little less time for the firewall to reach the Cisco cloud based on network conditions and the firewall model you are working with.

LED Status	Description	Time After Device Powered On (minutes:seconds)
Fast flashing green Seen on Status or SYS LED on all models.	The device is booting up correctly.	01:00
Fast flashing amber Seen on Status or SYS LED on all models.	The device failed to boot correctly.	01:00
Solid green Seen on Status or SYS LED on all models.	The application is loaded on the device.	10:00
Solid amber Seen on Status or SYS LED on all models.	The application failed to load correctly on the device.	10:00
Slow flashing green Seen on Status or SYS LED on Firepower 1000 and Firepower 2100 series devices. Seen on M LED of Secure Firewall 3100 series devices.	The device is connected to the Cisco cloud.	15:00
Alternating green and amber Seen on Status or SYS LED on Firepower 1000 and Firepower 2100 series devices. Seen on M LED of Secure Firewall 3100 series devices.	The device failed to connect to the Cisco cloud.	15:00

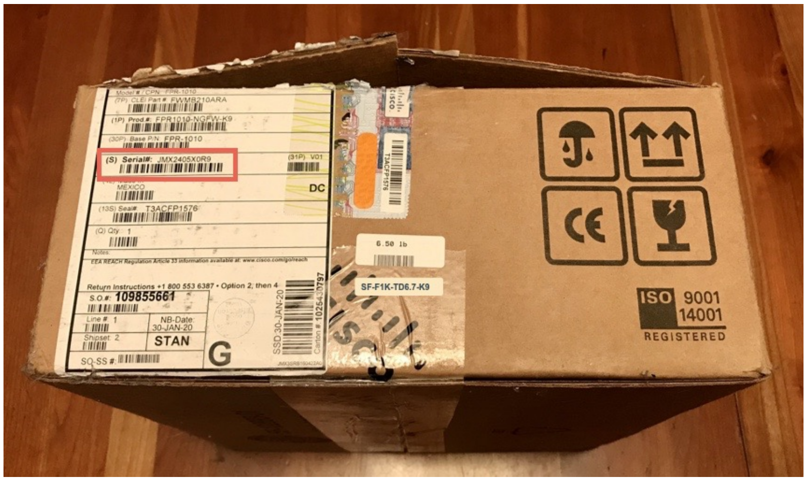
After you complete this task, locate and supply the device's serial number to your IT administrator. The IT admin will configure the firewall remotely.

Find Your Device's Serial Number

Your IT department needs your firewall's serial number to connect to the device and manage it remotely. You can find the serial number in two different places.

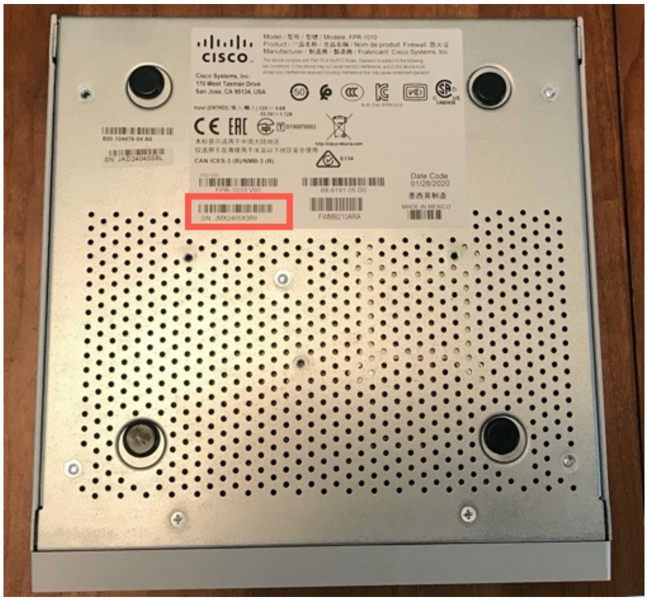
The Label on the Shipping Carton

The serial number is printed on the label on the shipping carton the firewall came in. Here is an example:

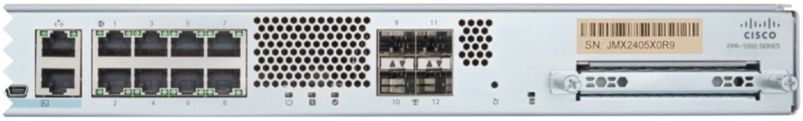


The Label on the Chassis

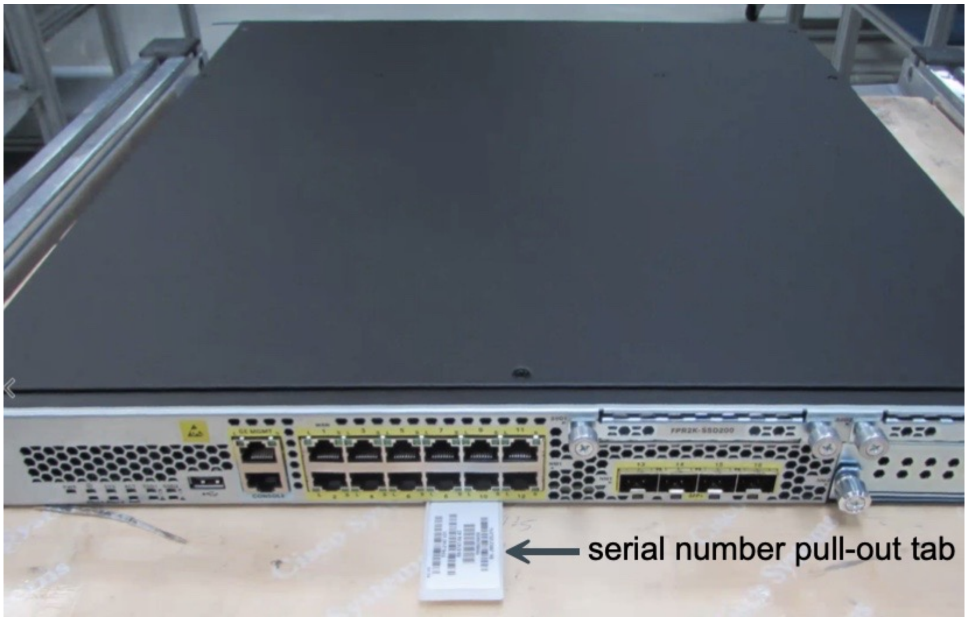
Firepower 1000: The serial number is on a label on the bottom of the device.



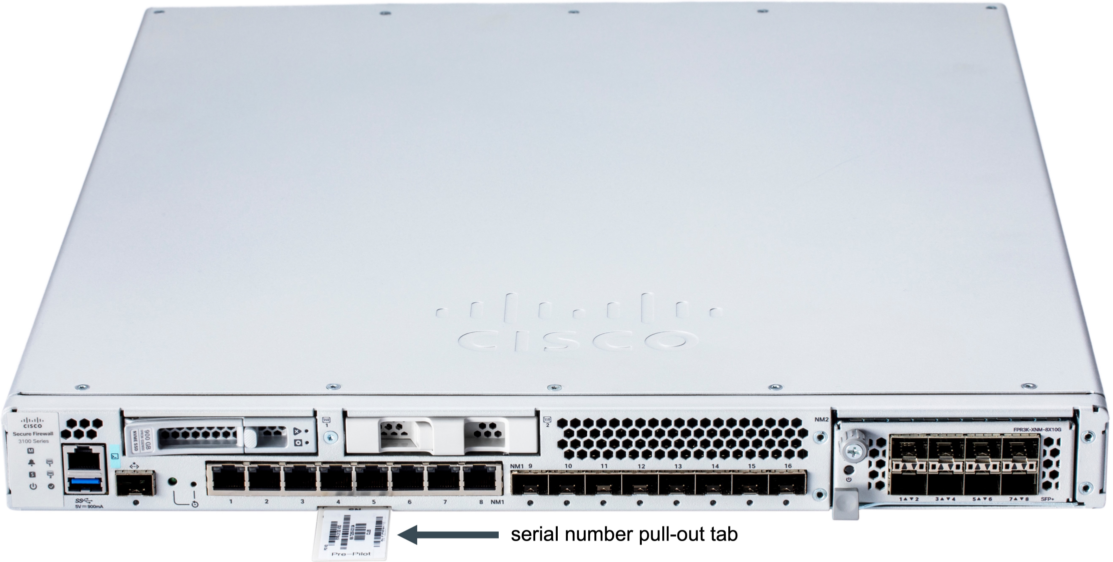
Firepower 1100: The serial number is on a label on the back of the device or on the bottom of the device.



Firepower 2100: The serial number is on a label on a pull-out tab on the front of the device.



Secure Firewall 3100:The serial number is on a label on a pull-out tab on the front of the device.



(Optional) Connect to the Firewall Using a Console Cable

You can connect a console cable from a device such as a laptop to your firewall, open up a terminal window, and enter a few commands to display the device's serial number.

Note This procedure connects a computer to the firewall using a console cable in order to retrieve the device's serial number, it is for advanced users who are comfortable working with a command line interface and, possibly, installing software drivers on their laptops.

1. See Connect to the Console Port for instructions on how to connect a laptop to your device using a console cable. Though the commands are explained in the Firepower 1010 Hardware Installation Guide, they are the same for all devices in the Firepower 1000 series, Firepower 2100 series, and Secure Firewall 3100 series devices

   There are two types of console ports for the 1010 and 1100 series devices. You can use either the USB-A to B console cable that came with the firewall or a DB-9 to RJ-45 serial cable.

   There is one console port on 2100 and 3100 series devices. These devices ship with only a DB-9 to RJ-45 serial cable. When using the cable, you need a third party serial-to-USB cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system.

2. Log in to the device as the admin user. If the device has not been configured, you are asked to create a new password for the admin.

3. At the `firepower#` prompt, enter `show chassis detail`. Here is an example of the output from a 1010 series device. Your device's model number will be listed in the **Product Name** field:

   ```
   firepower# show chassis detail

   Chassis:
       Chassis: 1
       Overall Status: Operable
       Oper qualifier: N/A
       Operability: Operable
       Product Name: Cisco Firepower 1010 Security Appliance
       PID: FPR-1010
       VID: V01
       Vendor: Cisco Systems, Inc
       Serial (SN): JMX2405X0R9
       HW Revision: 0.6
       PCB Serial Number: JAD24040S6L
       Power State: Ok
       Thermal Status: Ok
       Boot Status: OK
       Current Task:
   firepower#
   ```

   The output shows two serial numbers. You **must** report the value of the Serial (SN) field to your IT department to complete the onboarding process.

Administrator: Onboard a Device to CDO

If you are a CDO administrator and someone at a branch office has connected an already configured 1000, 2100, or 3100 series device to their network, and your job is to onboard it to CDO using its serial number, see the procedure below.

If you are a CDO administrator and your task is to onboard *a fully configured new* Cisco Firepower 1000, 2100, or Secure Firewall 3100 series device, use either the CLI registration key or serial number method that does not use low-touch-provisioning to onboard the device. Read and review these procedures in the Managing FDM Devices with Cisco Defense Orchestrator guide to determine whether these procedures are more applicable for your scenario.

Onboard a Secure Firewall Threat Defense to CDO Using Its Serial Number

If you are a CDO administrator and someone at a branch office has connected a *new and unconfigured*, Cisco Firepower 1000, 2100, or Secure Firewall 3100 series device to their network, and your job is to onboard it to CDO using its serial number, we strongly recommend using low-touch provisioning to onboard the device.

Ensure the device has the following environment:

- The device has at least veriosn 7.2 installed. To use the CLI to check the software version, and to install a new version, see the getting started guide for your model.
- The device must be new and unconfigured, or freshly instealled with at least version 7.2.

Procedure

Step 1 Log in to CDO.

Step 2 In the navigation pane, click **Inventory** and click the blue plus button.

Step 3 Select the **FTD** tile.

Step 4 Under **Management Mode**, be sure **FTD** is selected.

At any point after selecting **FTD** as the management mode, you can click **Manage Smart License** to enroll in or modify the existing smart licenses avialable for your device. If you currently do not have any smart licenses available for your tenant, you can opt for the **90-day Evaluation License**. If you have already activated the 90-day evaluation mode, the onboarding wizard displays how many days are left.

Step 5 Enter the **Device Serial Number** and the **Device Name**. Select **Next**.

Step 6 **Password Reset.** Select the **Yes, this new device has never been logged into or configured for a manager** option.

Step 7 Click **Next**.

Step 8 In the Policy Assignment step, use the drop-down menu to select an access control policy to deploy once the device is onboarded. If you have no policies configured, select the **Default Access Control Policy**.

Step 9 Select the base licenses you want applied to the device. Click **Next**.

What to do next

From the **Inventory** page, select the device you just onboarded and select any of the option listed under the **Management** pane located to the right. We strongly recommend the following actions:

- Create a custom access control policy to customize the security for your environment. See the *Access Control Policies* chapter for more information.
- Enable Cisco Security Analytics and Logging (SAL) to view events in the CDO dashboard **or** register the device to an Firepower Management Center for security analytics. See the *Cisco Security Analytics and Logging* chapter for more information.

Remote Branch Office Deployment of Secure Firewall Threat Defense Devices for Management by the Firepower Management Center

You can deploy the Secure Firewall Threat Defense device low-touch provisioning for CDO customers and remote branch deployment for Firepower Management Center users.

Use one of the following methods to provision your device:

- An administrator at the central headquarters pre-configures the device at the CLI or using the threat defense device manager, and then sends the device to the remote branch office.
- The branch office administrator cables and powers on the device.
- The central administrator completes configuration of the device using the Firepower Management Center.

See the getting started guide for your model for more information:

- Cisco Firepower 1010
- Cisco Firepower 1100
- Cisco Firepower 2100
- Secure Firewall 3100

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.

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.