

Cisco Firepower 1000、2100、および Secure Firewall 3100 シリーズの簡単導入ガイド

初版：2020年10月28日

最終更新：2022年4月7日

Cisco Firepower 1000、2100、および Secure Firewall 3100 シリーズの簡単導入ガイド

このドキュメントでは、次のモデルについて、Firepower Threat Defense の2つの簡単な展開オプション、Cisco Defense Orchestrator 顧客向けのロータッチプロビジョニングと Firepower Management Center 顧客向けのリモートブランチオフィスの展開に関する情報を提供します。

- - FTD ソフトウェアバージョン 6.7 以降がインストールされている Firepower 1000 シリーズまたは Firepower 2100 シリーズのデバイス。
- - FTD ソフトウェアバージョン 7.1 以降がインストールされている Cisco Secure Firewall 3100 シリーズのデバイス。

CDO を使用したロータッチプロビジョニング


ロータッチプロビジョニングにより、誰でも新しい Firepower 1000、Firepower 2100、Cisco Secure Firewall 3100 シリーズデバイスをネットワークに接続できるため、IT 部門はデバイスを CDO にオンボーディングしてリモートで構成できます。

「何をしようとしていますか? (What do you want to do?)」。

- [新しい FTD をネットワークに接続する](#)。私はブランチオフィスで働いています。
- [シリアル番号を使用して FTD から Cisco Defense Orchestrator にオンボード](#)。私は CDO 管理者です。

新しい FTD をネットワークに接続する

ここでは、CDO 管理者がリモートで管理できるようにファイアウォールをネットワークに接続するプロセスについて説明します。

分散拠点でファイアウォールの通知を受け取ってネットワーク、に接続することが目的の場合は、[このビデオをご覧ください](#)。

ビデオでは、ファイアウォールについて、およびデバイスのステータスを示すデバイス上の LED シーケンスについて説明しています。IT 部門と一緒に LED を見るだけでデバイスのステータスを確認できます。ビデオで説明されている手順は次のとおりです。

1. デバイスに正しいソフトウェアがインストールされていることを確認します。デバイスが入っていた配送用の箱を確認してください。デバイスにインストールされている FTD ソフトウェアを識別する無地の白いステッカーが貼られているはずです。ソフトウェアパッケージ番号は、次の表のようになります。

| ロータチプロビジョニングをサポートするファイアウォールモデル番号 | サポート対象のファイアウォールソフトウェアバージョン | FTDソフトウェアパッケージ |
|--|----------------------------|-------------------|
| Firepower 1000 シリーズデバイス モデル：1010、1120、1140、1150 | 6.7 以降 | SF-F1K-TD6.7-K9 |
| Firepower 2100 シリーズデバイス モデル：2110、2120、2130、2140 | 6.7 以降 | SF-F2K-TD6.7-K9 |
| Cisco Secure Firewall 3100 シリーズ デバイスモデル：3110、 3120、3130、3140 | 7.1 以降 | SF-F3K-TD7.1.0-K9 |

2. デバイスをラックに収納するか、配送用の箱を処分する前に、デバイスのシリアル番号を記録して IT 部門に送信してください。シリアル番号はデバイス管理に必要です。デバイスのシリアル番号は、デバイスが入っていた配送用の箱と、デバイス自体に貼られたラベルに記載されています。詳細については、[デバイスのシリアル番号の確認 \(6 ページ\)](#) を参照してください。
3. 箱を開梱し、中身を取り出します。デバイスを設置してネットワークに接続し、デバイスが Cisco Cloud に正常に登録されるまで、配送用の箱を保管してください。
4. デバイスを電源に接続します。
5. イーサネット 1/1 インターフェイスから WAN モデムにネットワークケーブルを接続します。WAN モデムは、分散拠点とインターネットを接続する機器であり、ファイアウォールからインターネットへのルートにもなります。



(注) デバイスの管理インターフェイスから WAN にはネットワークケーブルを接続しないでください。

図 1: Firepower 1010 のケーブル配線

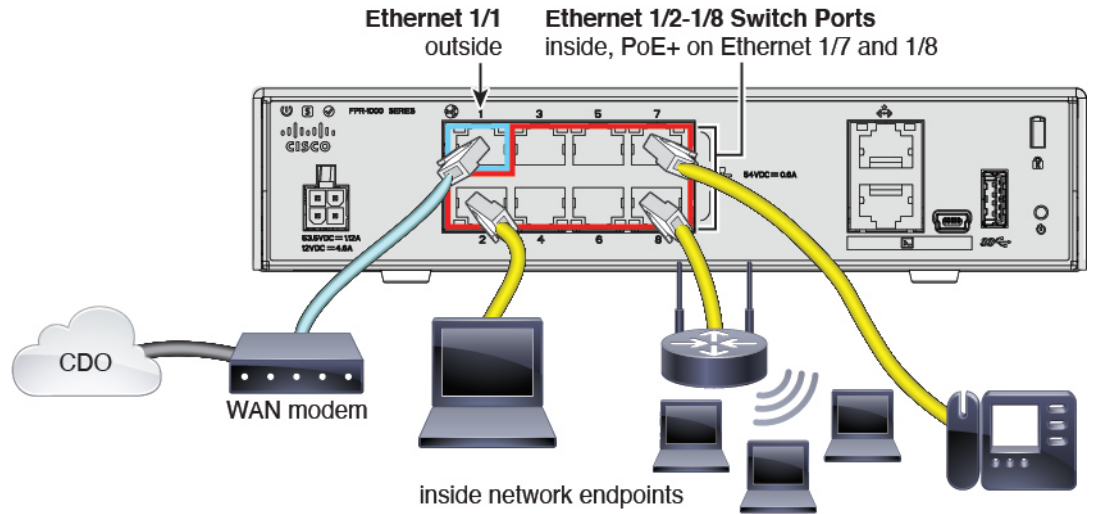


図 2: Firepower 1100 のケーブル配線

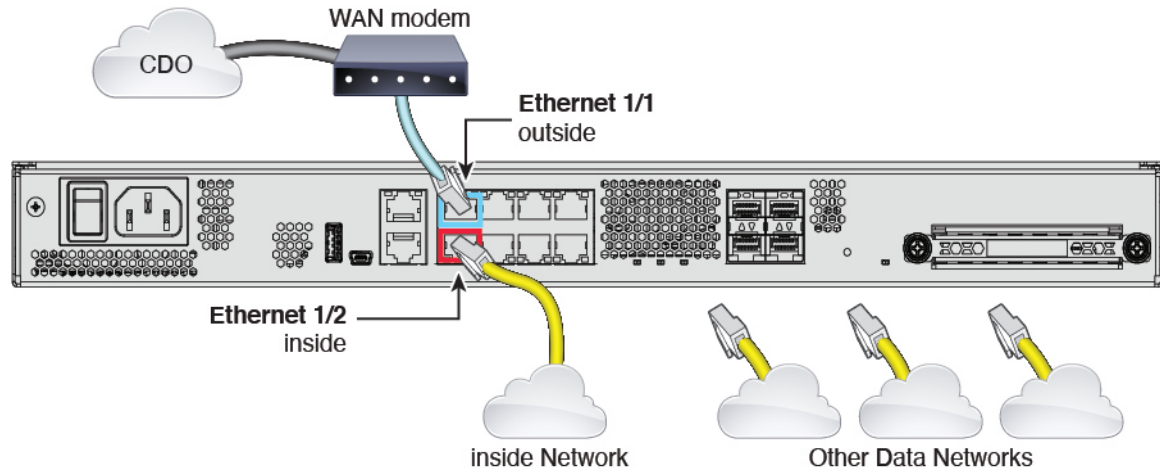


図 3: Firepower 2100 のケーブル配線

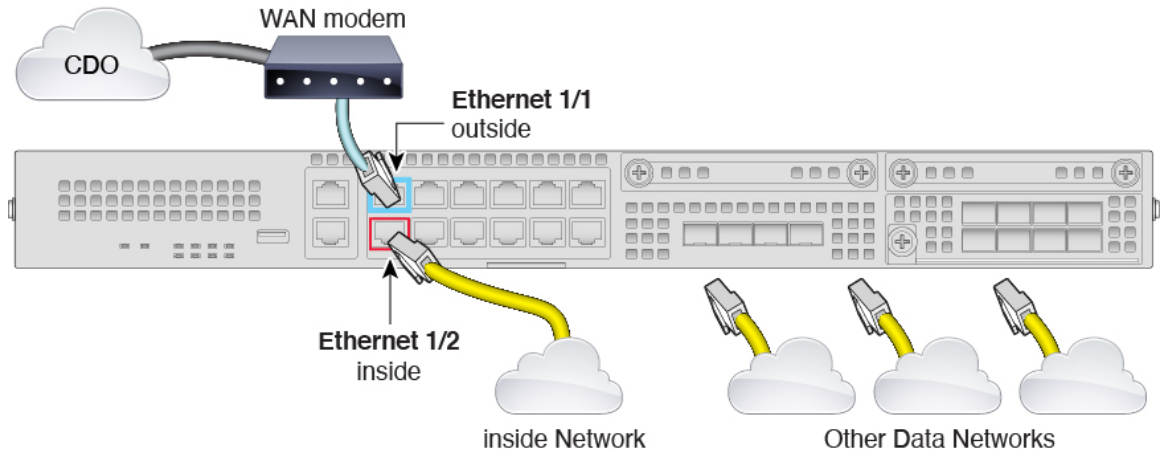
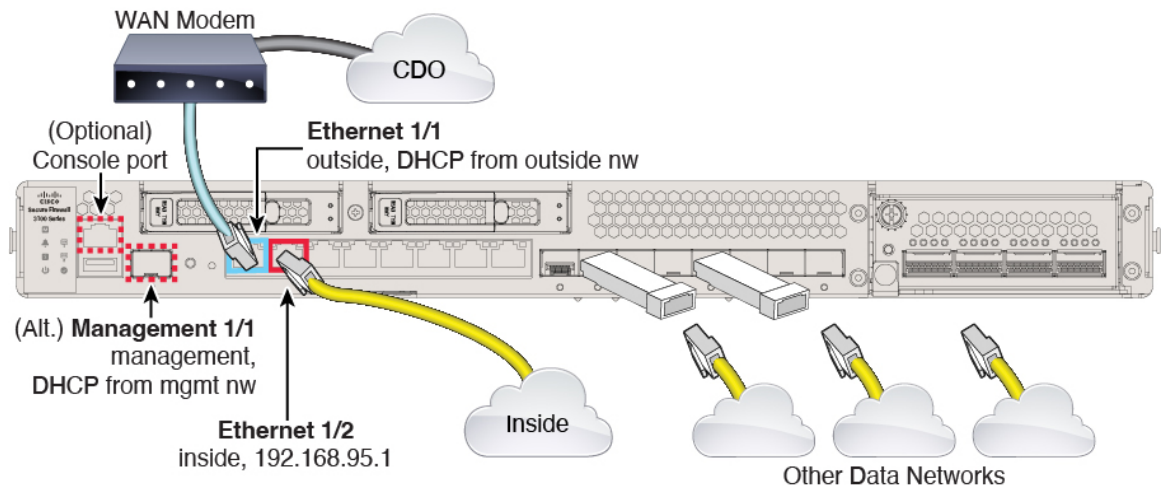


図 4: Cisco Secure Firewall 3100 のケーブル配線



6. デバイスのステータス LED、SYS LED、または MLED を観察して、デバイスが Cisco Cloud に到達したかどうかを判断します。次の表は、LED ステータスと、イーサネットケーブルを接続してから到達までのおおよその時間を示しています。ネットワークの状態や使用しているファイアウォールモデルによっては、ファイアウォールが Cisco Cloud に到達するまでに、もう少し時間がかかる場合があります。

| LED ステータス | 説明 | デバイスの電源を入れた後の時間 (分 : 秒) |
|---|------------------|-------------------------|
| 緑色で高速点滅 すべてのモデルのステータス LED または SYS LED で確認できます。 | デバイスは正しく起動しています。 | 01:00 |

| LED ステータス | 説明 | デバイスの電源を入れた後の時間（分：秒） |
|---|--------------------------------|----------------------|
| オレンジ色で高速点滅 すべてのモデルのステータス LED または SYS LED で確認できます。 | デバイスが正しく起動しませんでした。 | 01:00 |
| 緑色に点灯 すべてのモデルのステータス LED または SYS LED で確認できます。 | アプリケーションがデバイスにロードされました。 | 10:00 |
| オレンジに点灯 すべてのモデルのステータス LED または SYS LED で確認できます。 | アプリケーションがデバイスに正しく読み込まれませんでした。 | 10:00 |
| 緑色で低速点滅 Firepower 1000 および Firepower 2100 シリーズデバイスのステータス LED または SYS LED で確認できます。 Cisco Secure Firewall 3100 シリーズデバイスの M LED で確認できます。 | デバイスが Cisco Cloud に接続されました。 | 15:00 |
| グリーンとオレンジに交互に点滅 Firepower 1000 および Firepower 2100 シリーズデバイスのステータス LED または SYS LED で確認できます。 Cisco Secure Firewall 3100 シリーズデバイスの M LED で確認できます。 | デバイスが Cisco Cloud に接続できませんでした。 | 15:00 |

このタスクを完了すると、IT 管理者はファイアウォールをリモートから設定できるようになります。これで完了です。

シリアル番号を使用して FTD から Cisco Defense Orchestrator にオンボード

ユーザーが CDO 管理者であり、ブランチオフィスの誰かが新しい未構成の Cisco Firepower 1000、2100、または Cisco Secure Firewall 3100 シリーズデバイスをネットワークに接続している場合、ユーザーのタスクはそれを使用してデバイスを CDO にオンボードすることです。デバイスのシリアル番号を使用して FTD をオンボーディングする手順を参照してください。

ユーザーが CDO 管理者であり、完全に構成された新しい Cisco Firepower 1000、2100、または Cisco Secure Firewall 3100 シリーズデバイスをオンボードすることがタスクである場合、デバイスを CDO にオンボードする他の 2 つの方法は次の通りです。

- 登録キーを使用した FTD のオンボード
- デバイスのシリアル番号を使用した FTD の導入準備

デバイスのシリアル番号の確認

IT 部門では、デバイスに接続してリモートで管理するために、デバイスのシリアル番号が必要になります。シリアル番号は 2 か所で確認できます。

製品の梱包箱上のラベル

シリアル番号は、ファイアウォール製品の梱包箱のラベルに印刷されています。例を次に示します。

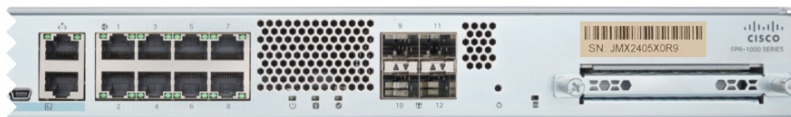


シャーシのラベル

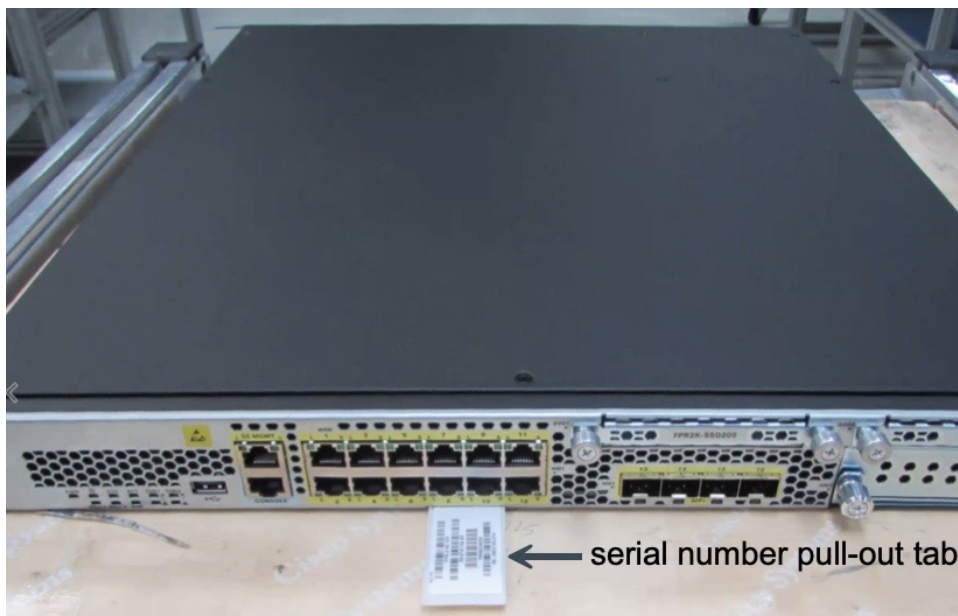
Firepower 1000 : シリアル番号は、デバイスの底面のラベルに記載されています。



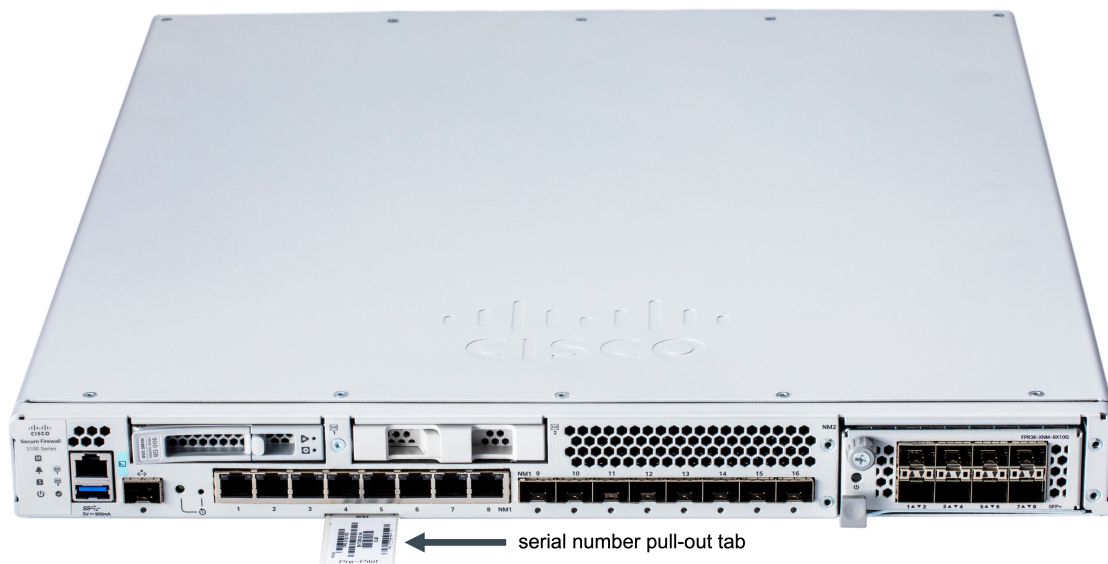
Firepower 1100 : シリアル番号は、デバイスの背面または底面のラベルに記載されています。



Firepower 2100 : シリアル番号は、デバイス前面の引き出しタブのラベルに記載されています。



Cisco Secure Firewall 3100 : シリアル番号は、デバイス前面の引き出しタブのラベルに記載されています。



(任意) コンソールケーブルを使用したファイアウォールへの接続

ラップトップなどのデバイスからファイアウォールにコンソールケーブルを接続し、ターミナルウィンドウを開いてコマンドをいくつか入力すると、デバイスのシリアル番号を表示できます。



(注) この手順では、コンソールケーブルを使用してコンピュータをファイアウォールに接続し、デバイスのシリアル番号を取得します。コマンドラインインターフェイスを使用したり、ラップトップにソフトウェアドライバをインストールしたりすることに慣れている上級ユーザー向けです。

1. コンソールケーブルを使用してラップトップをデバイスに接続する方法については、「[コンソールポートへの接続](#)」を参照してください。コマンドの説明は『Cisco Firepower 1010 ハードウェア設置ガイド』に記載されています。Firepower 1000 シリーズ、Firepower 2100 シリーズ、および Cisco Secure Firewall 3100 シリーズのすべてのデバイスでも同じです。

1010 および 1100 シリーズのデバイスには、2 種類のコンソールポートがあります。ファイアウォールに付属の USBA - B コンソールケーブルまたは DB9 - RJ45 シリアルケーブルを使用できます。

Firepower 2100 および 3100 シリーズのデバイスにはコンソールポートが 1 つあります。これらのデバイスには、DB9 - RJ45 シリアルケーブルのみが付属しています。ケーブルの接続には、サードパーティ製のシリアル - USB ケーブルが必要になる場合があります。ご使用のオペレーティングシステムに必要な USB シリアルドライバを必ずインストールしてください。

2. 管理ユーザーとしてデバイスにログインします。デバイスが設定されていない場合は、管理者用に新しいパスワードを作成するよう求められます。

3. firepower# プロンプトで、`show chassis details` と入力します。Firepower 1010 デバイスからの出力の例を次に示します。デバイスのモデル番号が [製品名 (ProductName)] フィールドに表示されます。

```
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#
```

出力には、2つのシリアル番号が表示されます。シリアル (SN) フィールドの値を IT 部門に報告してください。

FMC による管理用 FTD デバイスのリモートブランチオフィス展開

中央本社の FMC を使用して、リモートブランチオフィスに FTD を導入できます。

FTD をプロビジョニングするには、次のいずれかの方法を使用します。

- 本社の管理者は、CLI または FDM を使用して FTD を事前設定してから、リモートブランチオフィスに FTD を送信します。
- ブランチオフィスの管理者が、FTD をケーブルで接続して電源をオンにします。
- 中央管理者が、FMC を使用して FTD の設定を完了します。

詳細については、モデルのスタートガイドを参照してください。

- [Firepower 1010](#)
- [Firepower 1100](#)
- [Firepower 2100](#)
- [Cisco Secure Firewall 3100](#)

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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.

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.