

# Firepower Easy Deployment Guide for Cisco Firepower 1000 or 2100 Firewalls

---

**First Published:** 2020-10-28

**Last Modified:** 2021-05-18

## Firepower Easy Deployment Guide for Cisco Firepower 1000 or 2100 Firewalls

This document provides information about two easy deployment options for customers of Firepower Threat Defense (FTD) version 6.7 and later: Low-Touch Provisioning for Cisco Defense Orchestrator (CDO) customers and Remote Branch Office Deployment for Firepower Management Center (FMC) customers.

- See [Low-Touch Provisioning Using CDO, on page 1](#) if your job is to connect a new Firepower firewall to your network or to manage that new firewall with CDO.
- See [Remote Branch Office Deployment of FTD Devices for Management by an FMC, on page 7](#) if you are an FMC administrator and want to manage an FTD at a remote branch using FMC.

## Low-Touch Provisioning Using CDO


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

What do you want to do?

- [Connect a New Cisco Firepower Firewall to Your Network](#). I work at the branch office.
- [Onboard a Firepower Firewall to CDO Using its Serial Number](#). I am the CDO administrator.

## Connect a New Cisco Firepower Firewall to Your Network

This topic describes the process of connecting your Firepower firewall to your network so that it can be managed remotely by a CDO administrator.

If you received a Firepower firewall at your branch office and your job is to plug it in to your network, [watch this video](#). 

The video describes your firewall and the LED sequences on the device that indicate the device's status. If you need to, you'll be able to confirm the device's status with your IT department just by looking at the LEDs. These are the steps described in the video:

1. Your Firepower firewall needs to be one of a certain model number and needs to have FTD version 6.7 installed on it for low-touch provisioning to work. The table below shows the Firepower models that support low-touch provisioning.

To make sure the Firepower model has the right software installed, look on the cardboard box the device came in. It should have a plain white sticker on it with a product identifier that looks similar to one in the following table:

Firepower Model Numbers that Support Low-Touch Provisioning	FTD 6.7 Product Identifiers
Firepower 1000 series device models: 1010, 1120, 1140, 1150	SF-F1K-TD6.7-K9
Firepower 2100 series device models: 2110, 2120, 2130, 2140	SF-F2K-TD6.7-K9

- Before you rack the device or throw the cardboard box away, record your device's serial number and send it to your IT department. They will need it to manage the device. The serial number of the device is located on the cardboard box the device came in and on a sticker affixed to the device itself. See [Find Your Device's Serial Number](#), on page 4 for more information.
- Unpack the box and take inventory of the contents.  
Keep the cardboard box until you have plugged in the device, you have connected it to your network, and the device has successfully contacted the Cisco cloud.
- Connect the device to power.
- Connect the network cable from the Ethernet 1/1 interface to your wide area network (WAN) modem. Your WAN modem is your branch's connection to the internet and will be your Firepower 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**

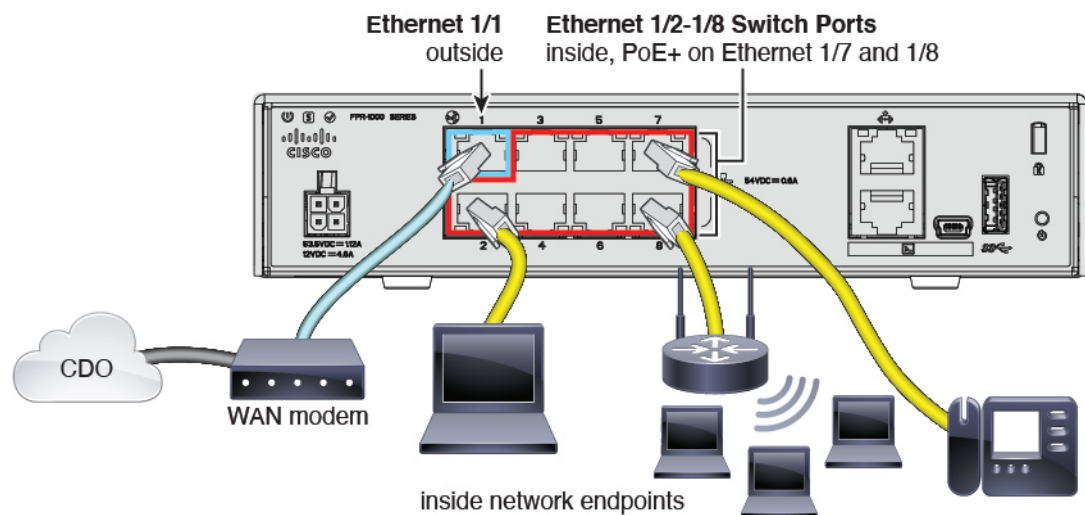


Figure 2: Firepower 1100 Cabling

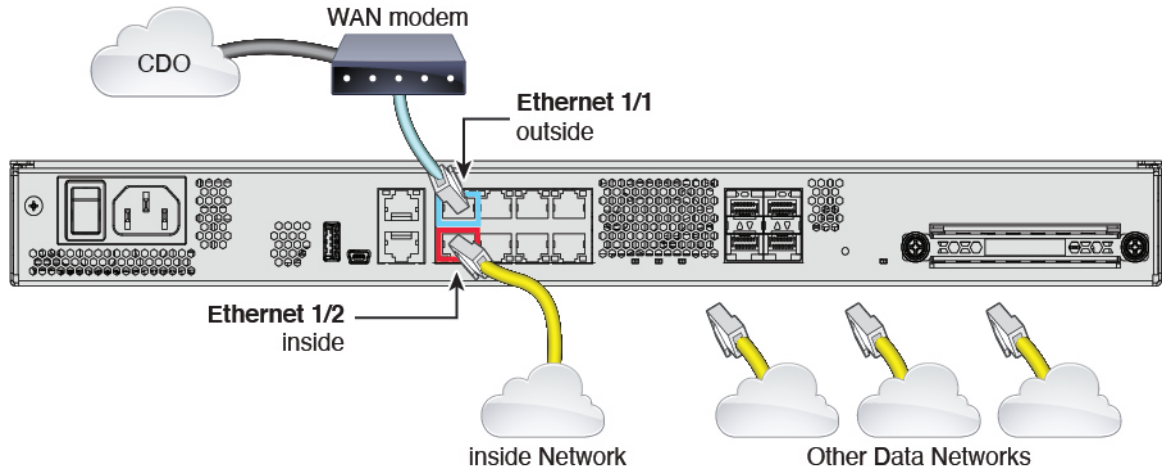
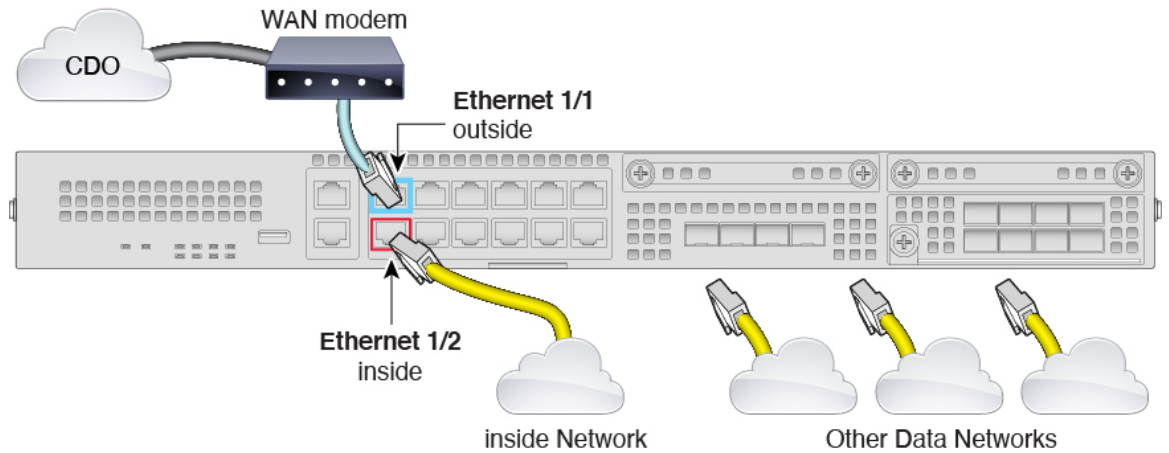


Figure 3: Firepower 2100 Cabling



- Observe the Status/SYS LED light pattern on the device to determine if the device has reached the Cisco cloud. The table below provides the LED light patterns and the approximate time they occur. It may take a little more time or a little less time for the Firepower device to reach the Cisco cloud based on network conditions and the Firepower model you are working with.

Light pattern of Status/SYS LED	Description	Time this occurs after the device is powered on. (minutes:seconds)
Fast flashing green	The device is booting up correctly.	01:00
Fast flashing amber	The device failed to boot correctly.	01:00
Solid green	The application is loaded on the device.	10:00

Light pattern of Status/SYS LED	Description	Time this occurs after the device is powered on. (minutes:seconds)
Solid amber	The application failed to load correctly on the device.	10:00
Slow flashing green	The device is connected to the Cisco cloud.	15:00
Alternating green and amber	The device failed to connect to the Cisco cloud.	15:00

After you complete this task, your IT administrator will be able to configure the firewall remotely. You're done.

## Onboard a Firepower Firewall to CDO Using its Serial Number

If you are a Cisco Defense Orchestrator (CDO) administrator and someone at a branch office has connected a *new* Cisco Firepower firewall running Firepower Threat Defense version 6.7 or later device to their network, and your job is to onboard it to CDO using its serial number, see [Procedure for Onboarding an FTD using the Device's Serial Number](#)

If you are a CDO administrator and your task is to onboard a *fully configured* Cisco Firepower firewall running Firepower Threat Defense 6.7 or later, here are two other methods of onboarding the device to CDO:

- [Onboard an FTD Using a Registration Key](#)
- [Onboard an FTD Using the Device's Serial Number](#)

## Find Your Device's Serial Number

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

### The Sticker on the Cardboard Box

The serial number is printed on the sticker on the cardboard box the firewall came in. Here is an example:

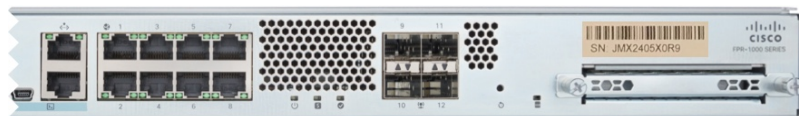


**The Sticker on the Chassis**

**Firepower 1010:** The serial number is on a sticker on the bottom of the device:



**Firepower 1100:** The serial number is on a sticker on the back of the device or on the bottom of the device:



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



### Connecting to the Firewall Using a Console Cable

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



#### Note

This procedure is for advanced users who are comfortable working with a command line interface and, possibly, installing software drivers on their laptops. Here is the procedure to connect a computer to the Firepower firewall using a console cable and to retrieve the device's serial number in a terminal window:

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 will be the same for the 1100 series devices and 2100 series devices.

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

The Firepower 2100 ships with only a DB-9 to RJ-45 serial cable. When using this cable, you will 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 will be asked to create a new password for the admin.
3. At the `firepower#` prompt, type `show chassis detail`. Here is an example:

```
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. Report the value of Serial (SN) field to your IT department.

## Remote Branch Office Deployment of FTD Devices for Management by an FMC

You can deploy the Firepower Threat Defense (FTD) at a remote branch office using a Firepower Management Center (FMC) at a central headquarters.

- An administrator at the central headquarters pre-configures the FTD at the CLI, and then sends the FTD to the remote branch office.
- The branch office administrator cables and powers on the FTD.
- The central administrator completes configuration of the FTD using the FMC.

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

- [Firepower 1010](#)
- [Firepower 1100](#)
- [Firepower 2100](#)

---

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 NON-INFRINGEMENT 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](http://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.