Easy Deployment for Cisco Secure Firewall Threat Defense Using Security Cloud Control

First Published: 2020-10-12

Last Modified: 2026-11-03

Easy Deployment for Cisco Secure Firewall Threat Defense Using Security Cloud Control

Onboard the Firewall Threat Defense using zero-touch provisioning for management by Cloud-Delivered Firewall Management Center in Security Cloud Control.

For details about the end-to-end process of zero-touch provisioning of a Firewall Threat Defense, watch this video.

Prerequisites for easy deployment

Model support

This document is targeted at the following device models and versions. Examine the shipping carton in which the device arrived. It should have a white sticker identifying the software installed on the device.

Lists supported models and the accompanying software versions that support zero-touch provisioning.

Model	Version	Version shown on sticker
Secure Firewall 200	10.0 or later	SF-200-TDxx.x-K9 For example, SF-200-TD10.0-K9
Firepower 1010	7.2 or later	SF-F1K-TDx.x.x-K9 For example, SF-F1K-TD7.7.0-K9
Firepower 1100	7.2 or later	SF-F1K-TDx.x.x-K9 For example, SF-F1K-TD7.7.0-K9
Secure Firewall 1210/1220	7.6 or later	SF-F1200-TDx.x.x-K9 For example, SF-F1200-TD7.7.0-K9
Secure Firewall 1230/1240/1250	7.7 or later	SF-F1200-TDx.x.x-K9 For example, SF-F1200-TD7.7.0-K9
Firepower 2100	7.2, 7.3, or 7.4 (final supported version)	SF-F2K-TDx.x.x-K9 For example, SF-F2K-TD7.4.1-K9

Model	Version	Version shown on sticker
Secure Firewall 3100	7.2 or later	SF-F3K-TDx.x.x-K9 For example, SF-F3K-TD7.7.0-K9

Check if you need to reimage your device

If your device is not already running Firewall Threat Defense on a version compatibile with zero-touch provisioning, you can reimage the device. See the appropriate getting started guide for your device model, which tells you how to determine your operating system and version. You can also refer directly to the *Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*.

- Secure Firewall 200 getting started guide
- Firepower 1010 getting started guide.
- Firepower 1100 getting started guide.
- Secure Firewall 1210/1220 getting started guide
- Secure Firewall 1230/1240/1250 getting started guide
- Firepower 2100 getting started guide.
- Secure Firewall 3100 getting started guide.

Ensure zero-touch provisioning is enabled

Zero-Touch Provisioning is intended for devices that are in a factory-state only. Preconfiguration can prevent onboarding using the zero-touch provisioning method. If in doubt, you can restore its default state by pressing the small, recessed Reset button for longer than five seconds.

Branch office: connect the firewall to the internet

When you receive the firewall at your branch office, your job is to plug it in to your network. Watch this video.

The video displays unpacking your firewall and describes the LED sequences on the firewall that indicate the firewall's status while it gets deployed. These are the steps described in the video:

1. Examine the shipping carton in which the firewall arrived. It should have a white sticker identifying the **software installed** on the firewall. See Prerequisites for easy deployment, on page 1 for supported models and versions.
2. Before racking the firewall or discarding the shipping carton, record the firewall's **serial number** and share it with your IT department for management purposes. The serial number of the firewall is located on the shipping carton the firewall came in and on a label affixed to the firewall itself. See Find the firewall's serial number, on page 4 for more information.
3. Unpack the box and take inventory of the contents. Keep the shipping carton until you have plugged in the firewall, you have connected it to your network, and the firewall has successfully contacted the Cisco cloud.

4. Connect the firewall to **power**.
5. Connect the network cable from the **Ethernet 1/1** interface of your firewall to the **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 firewall's Management interface to your WAN.

6. Check the **LEDs** to determine when the firewall is ready for onboarding.

All models

Table 1: Initial startup: System (S or SYS) LED behavior

S or SYS LED	Description	Time after firewall powered on (minutes:seconds)
Fast flashing green	The firewall is booting up correctly.	01:00
Fast flashing amber (error condition)	The firewall failed to boot correctly.	01:00
Solid green	The application is loaded on the firewall.	10:00
Solid amber (error condition)	The application failed to load correctly on the firewall.	10:00

1010, 1100, 2100

Table 2: Zero-Touch Provisioning: System (S) LED behavior

S LED	Description	Time after firewall powered on (minutes:seconds)
Slow flashing green	Connected to the Cisco cloud and ready for onboarding	15:00 - 30:00
Alternating green and amber (error condition)	Failed to connect to the Cisco cloud	15:00 - 30:00

200, 1200, 3100

Table 3: Zero-Touch Provisioning: Managed (M) LED behavior

M LED	Description	Time after firewall powered on (minutes:seconds)
Slow flashing green	Connected to the Cisco cloud and ready for onboarding	15:00 - 30:00

M LED	Description	Time after firewall powered on (minutes:seconds)
Alternating green and amber (error condition)	Failed to connect to the Cisco cloud	15:00 - 30:00
Solid green	Onboarded	20:00 - 45:00

If you experience any error conditions, contact your IT department.

Find the firewall's serial number

Your IT department needs your firewall's serial number to onboard the firewall remotely. You can find the serial number in three different places.

The label on the shipping carton

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



The label on the chassis

Firepower 1010: The serial number is on a label at the bottom of the device.



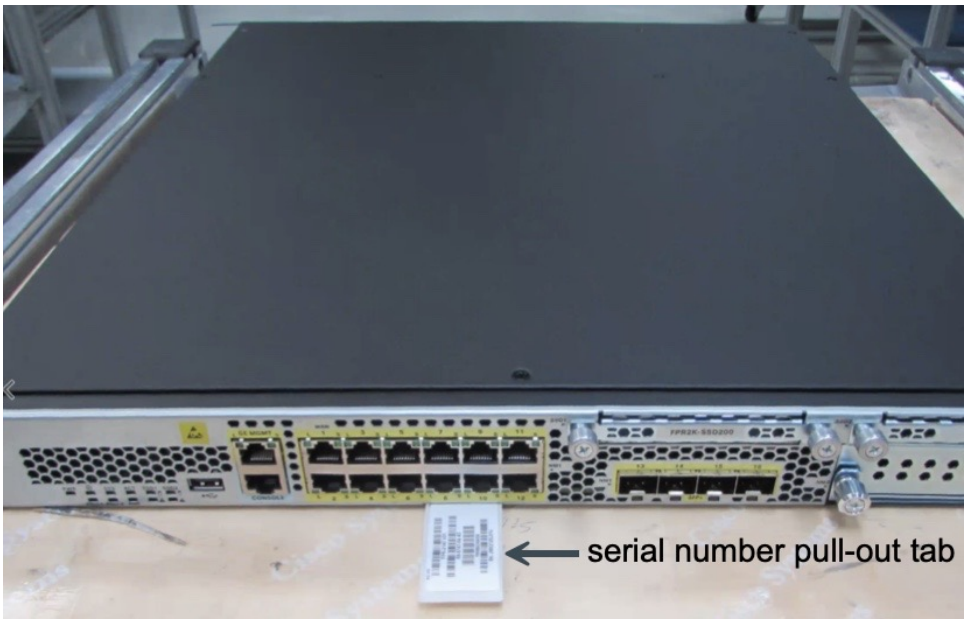
Firepower 1100: The serial number is on a label at the back of the device or at the bottom of the device.



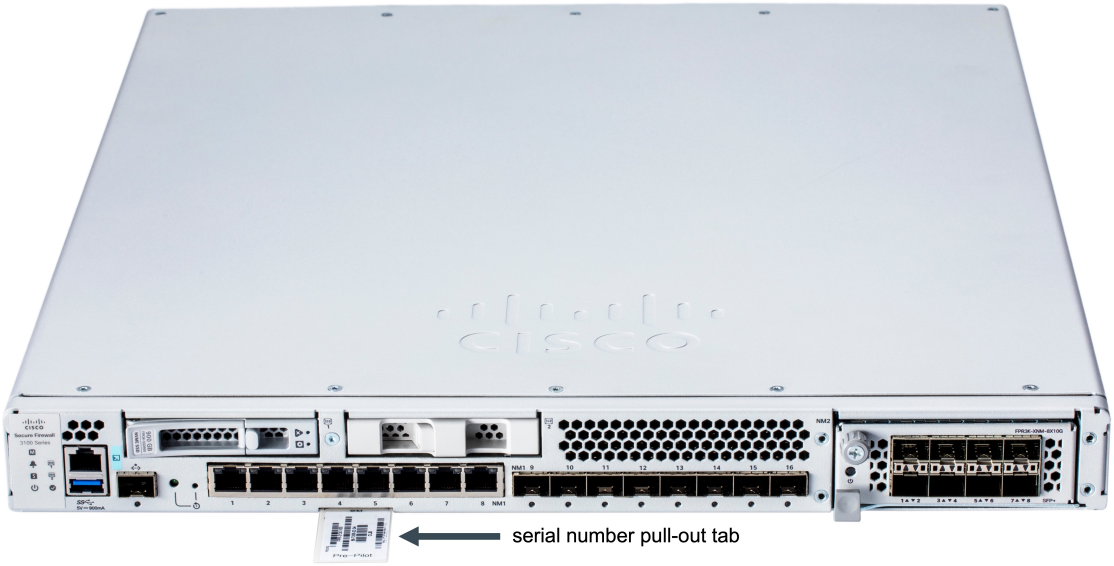
Secure Firewall 1210/1220: The serial number is on a label at the back of the device.



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



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



The CLI output on the console

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

Note This procedure causes you to set a new password. When your IT department onboards the firewall, be sure to specify that you already set the password.

1. See the getting started guide for your model for instructions on how to connect a laptop to your firewall using a console cable.
2. Log in to the device as the **admin** user. You need to enter the default password if this is your first login attempt: **Admin123**. You will then be prompted to change the password.
3. At the `firepower#` prompt, enter `show chassis detail`. Here is an example of the output from a 1010. Look for the **Serial Number (SN)** 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 should provide the **Serial (SN)** field to your IT department to complete the onboarding process. We don't recommend using the PCB serial number, although it may work. It's preferable to be consistent in using one type of serial number.

Alternatively, you can view the chassis serial number at the Firewall Threat Defense CLI using the **show inventory** command.

Onboard the firewall to the Cloud-Delivered Firewall Management Center using zero-touch provisioning

After the branch office connects the firewall to the internet, the IT administrator can onboard the firewall using the following procedure.

Procedure

Step 1 Log in to Security Cloud Control.

Step 2 In the left pane, click **Security Devices**.

Step 3 Click the **Onboard a device or service** ( ) icon to add a new device.

Step 4 Click the **FTD** tile.

Step 5 Under **Management Mode**, ensure you select **FTD**.

Step 6 Click the **Use Serial Number** tile.

Step 7 From the **Select FMC** drop-down list, choose **Cloud-Delivered FMC** and click **Next**.

Step 8 In the **Connection** step, enter the **Device Serial Number** and the **Device Name**.

Step 9 Click **Next**.

Step 10 In the **Password Reset** step, choose an option depending on whether the device was logged into and had the default-password changed or not:

- Default password — Click **Yes, this new device has never been logged into or configured for a manager**.
- Changed password — Click **No, this device has been logged into and configured for a manager**.

Step 11 Click **Next**.

Step 12 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 13 Click **Next**.

Step 14 Select the subscription licenses you want to apply to the device and click **Next**.

Step 15 In the **Done** step, click **Go to Security Devices** to go back to the **Security Devices** page.

What to do next

Once the device is synchronized, select the device you just onboarded from the **Security Devices** page and select any of the options listed under the **Device Management** pane located to the right. We strongly recommend the following actions:

- If you did not already, create a custom access control policy to customize the security for your environment. See Access Control Overview in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Firewall in Security Cloud Control for more information.
- Enable Cisco Security Analytics and Logging (SAL) to view events in the Security Cloud Control dashboard or register the device to an Secure Firewall Management Center for security analytics. See Cisco Security Analytics and Logging in Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Firewall in Security Cloud Control for more information.

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)

© 2025 Cisco Systems, Inc. All rights reserved.