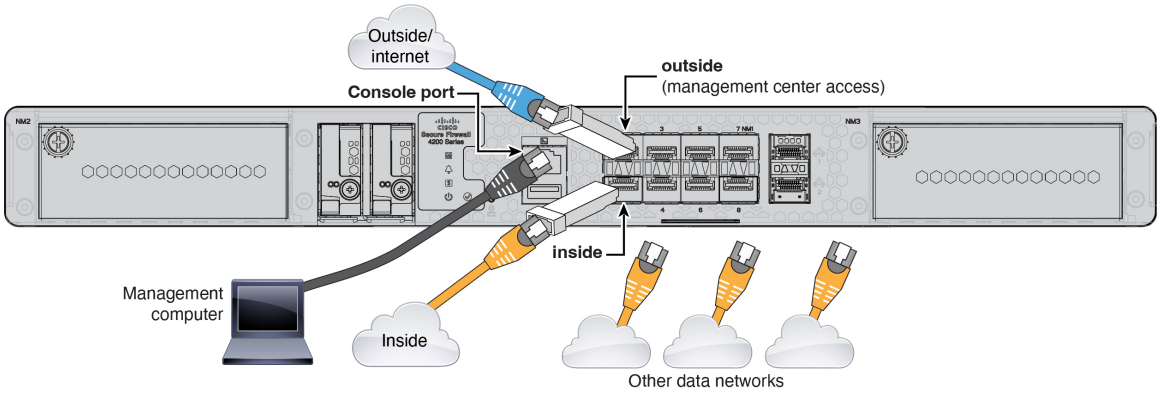
Cable and Register the Firewall

Cable the firewall and then register the firewall to the management center.

Cable the Firewall

- Obtain a console cable—The firewall does not ship with a console cable by default, so you will need to buy a third-party USB-to-RJ-45 serial cable, for example.
- Install SFPs into the data interface ports—The built-in ports are 1/10/25-Gb SFP28 ports that require SFP/SFP+/SFP28 modules.
- See the hardware installation guide for more information.



Perform Initial Configuration (Manual Provisioning)

For manual provisioning, perfom initial configuration of the firewall using the Secure Firewall device manager or using the CLI.

Initial Configuration: Device Manager

Using this method, after you register the firewall, the following interfaces will be preconfigured in addition to the Management interface:

- Ethernet 1/1—**outside**, IP address from DHCP, IPv6 autoconfiguration
- — **inside**, 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface
- Additional interfaces—Any interface configuration from the device manager is preserved.

Other settings, such as the DHCP server on inside, access control policy, or security zones, are not preserved.

Procedure

Step 1 Connect your computer to the inside interface.

Step 2 Log into the device manager.

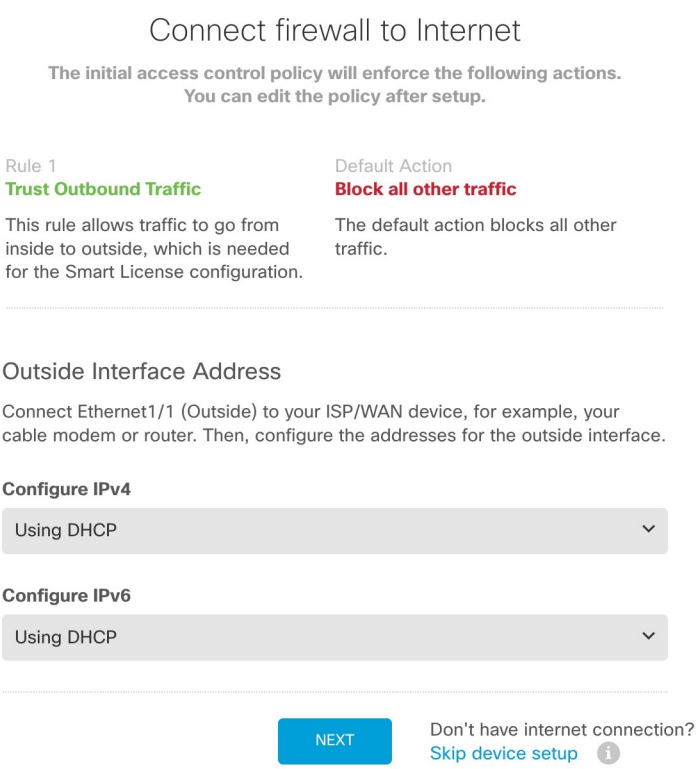
a) Go to https://192.168.95.1.
b) Log in with the username **admin** and the default password **Admin123**.
c) You are prompted to read and accept the General Terms and change the admin password.

Step 3 Use the setup wizard.

Note The exact port configuration depends on your model.

a) Configure the outside and management interfaces.

Figure 1: Connect firewall to internet



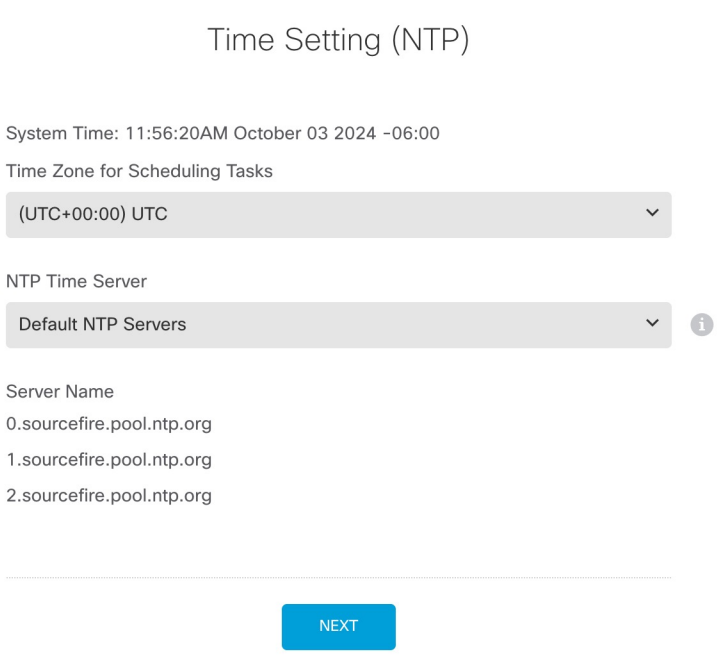
1. **Outside Interface Address**—Use a static IP address if you plan for high availability. You cannot configure PPPoE using the setup wizard; you can configure PPPoE after you complete the wizard.
2. **Management Interface**—The Management interface settings are used even though you are using manager access on the outside interface. For example, management traffic that is routed over the backplane through the outside interface will resolve FQDNs using these Management interface DNS servers, and not the outside interface DNS servers.

   DNS Servers—The DNS server for the system's management address. The default is the OpenDNS public DNS servers. These will probably match the outside interface DNS servers you set later since they are both accessed from the outside interface.

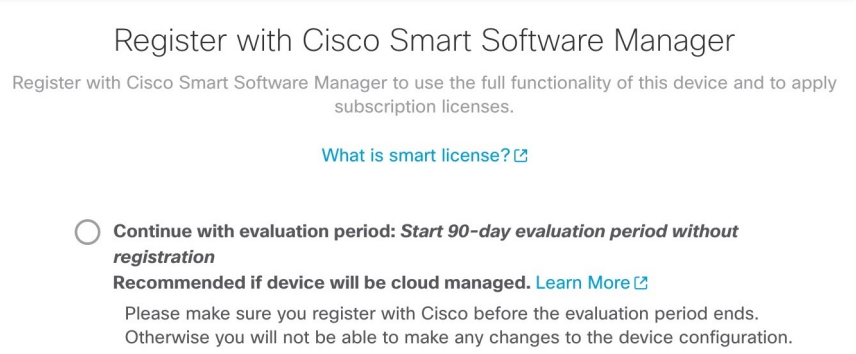
   Firewall Hostname

b) Configure the **Time Setting (NTP)** and click **Next**.

Figure 2: Time Setting (NTP)



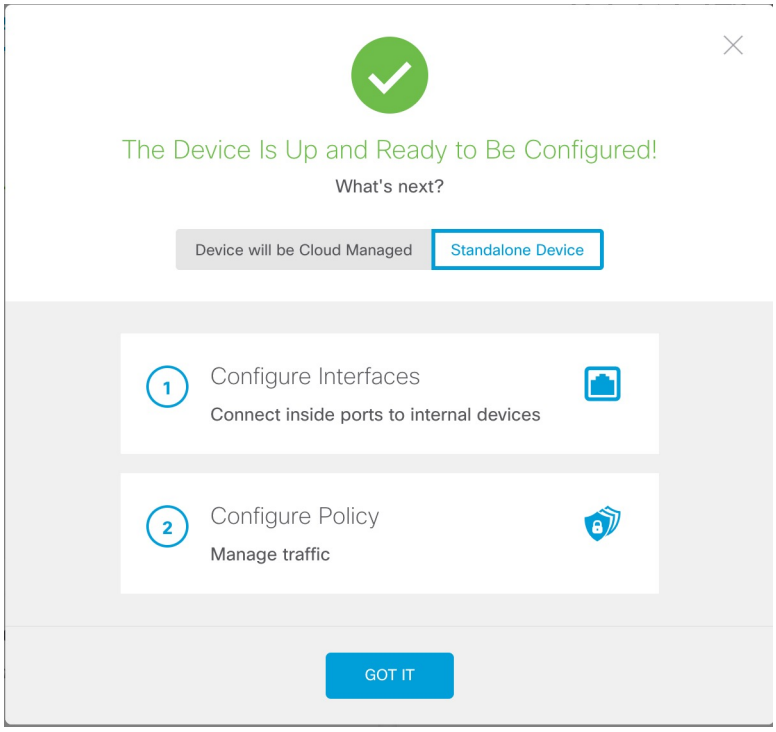
c) Select **Start 90 day evaluation period without registration**.



Do not register the threat defense with the Smart Software Manager; all licensing is performed on the management center.

d) Click **Finish**.

Figure 3: What's Next



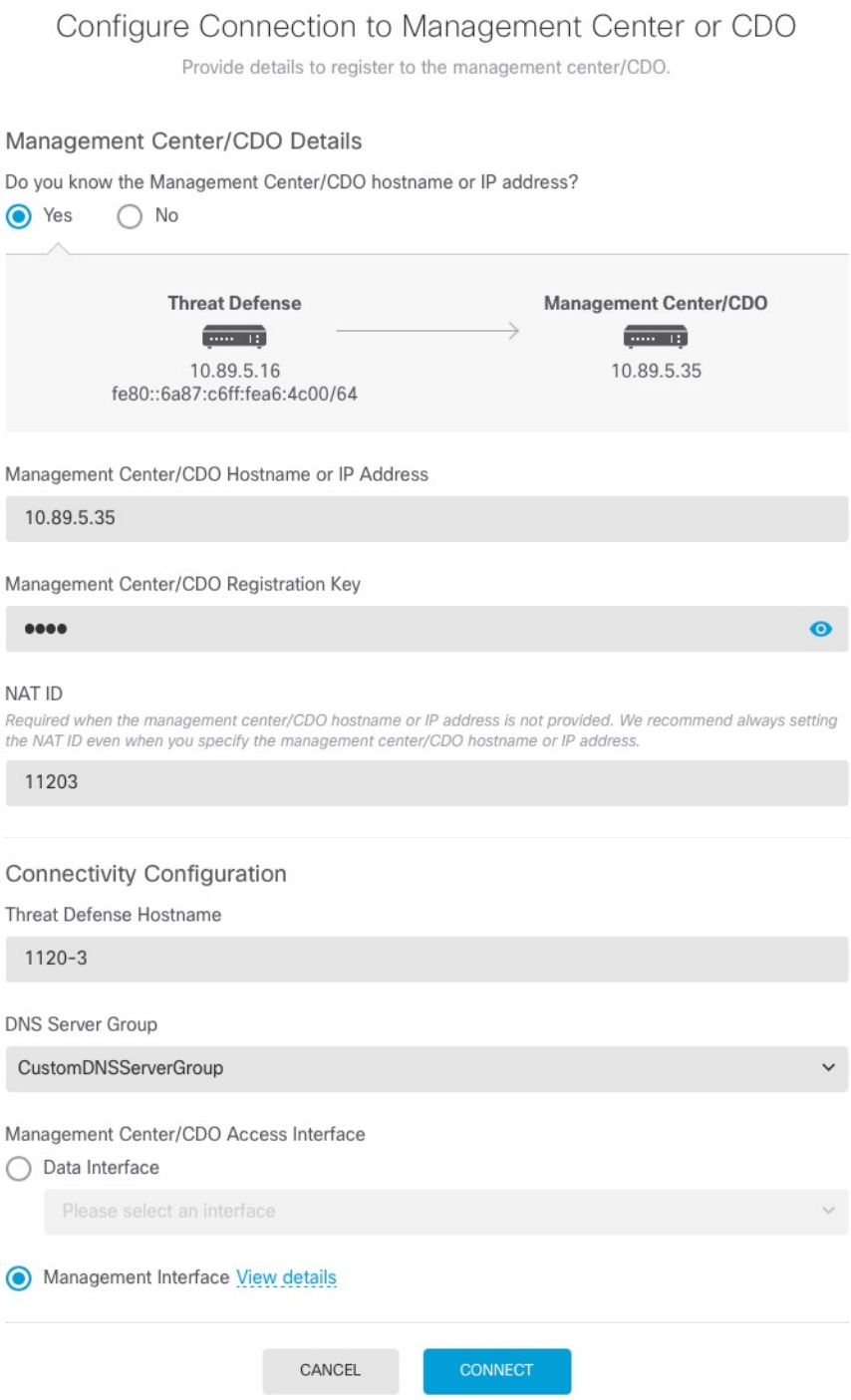
e) Choose **Standalone Device**, and then **Got It**.

Step 4 If you want to configure additional interfaces, choose **Device**, and then click the link in the **Interfaces** summary.

Step 5 Register with the management center by choosing **Device** > **System Settings** > **Central Management** and clicking **Proceed**

Configure the **Management Center/CDO Details**.

Figure 4: Management Center/CDO Details



a) For **Do you know the Management Center/CDO hostname or IP address**, click **Yes** if you can reach the management center using an IP address or hostname or **No** if the management center is behind NAT or does not have a public IP address or hostname.
b) If you chose **Yes**, enter the **Management Center/CDO Hostname/IP Address**.

c) Specify the **Management Center/CDO Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the management center when you register the firewall. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple firewalls registering to the management center.

d) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the management center. We recommend that you specify the NAT ID even if you know the IP addresses of both devices. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID *cannot* be used for any other firewalls registering to the management center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked.

Step 6 Configure the **Connectivity Configuration**.

a) Specify the **Threat Defense Hostname**.

This FQDN will be used for the outside interface.

b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

To retain the outside DNS server setting after registration, you need to re-configure the DNS Platform Settings in the management center.

c) For the **Management Center/CDO Access Interface**, click **Data Interface**, and then choose **outside**.

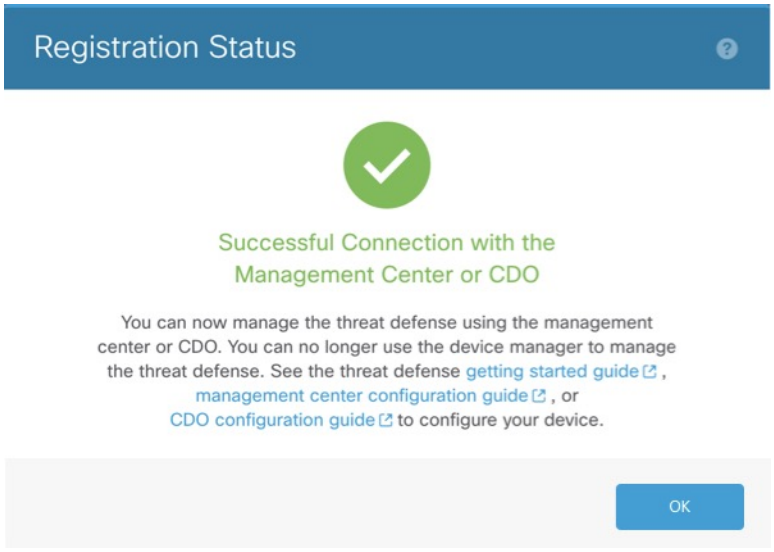
Step 7 (Optional) Click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the management center can reach the threat defense at its FQDN if the threat defense's IP address changes.

Step 8 Click **Connect**.

The **Registration Status** dialog box shows the current status of the management center registration.

Figure 5: Successful Connection



Step 9 After the **Saving Management Center/CDO Registration Settings** step on the status screen, go to the management center and add the firewall. See Register the Firewall with the Management Center Using Manual Provisioning, on page 14.

Initial Configuration: CLI

Set the dedicated Management IP address, gateway, and other basic networking settings using the CLI setup script.

Procedure

Step 1 Connect to the console port and access the threat defense CLI. See Access the Threat Defense CLI.

Step 2 Complete the CLI setup script for the Management interface settings.

Note You cannot repeat the CLI setup script unless you clear the configuration, for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See Cisco Secure Firewall Threat Defense Command Reference.

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
```

```
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
```

Guidance: Enter **y** for at least one of these types of addresses. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address.

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

Guidance: Choose **manual**. DHCP is not supported when using the outside interface for manager access. Make sure this interface is on a different subnet from the manager access interface to prevent routing issues.

```
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
```

Guidance: Set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the outside interface.

```
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
```

Guidance: Set the Management interface DNS servers. These will probably match the outside interface DNS servers you set later, since they are both accessed from the outside interface.

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

Guidance: Enter **routed**. Outside manager access is only supported in routed firewall mode.

```
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
```

```
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Step 3 Configure the outside interface for manager access.

configure network management-data-interface

You are then prompted to configure basic network settings for the outside interface.

Manual IP Address

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
```

Guidance: To retain the outside DNS servers after registration, you need to re-configure the DNS Platform Settings in the management center.

```
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the
manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

IP Address from DHCP

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the
manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Step 4 Identify the management center.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key nat_id*

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the management center. If the management center is not directly addressable, use **DONTRESOLVE**, in which case the firewall must have a reachable IP address or hostname.
- *reg_key*—Specifies a one-time registration key of your choice that you will also specify on the management center when you register the threat defense. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).
- *nat_id*—Specifies a unique, one-time string of your choice that you will also specify on the management center. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the management center.

Example:

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

Step 5 Shut down the threat defense so you can send the device to the remote branch office.

It's important that you shut down your system properly. Simply unplugging the power or pressing the power switch can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your system.

a) Enter the **shutdown** command.
b) Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).
c) After the chassis has successfully powered off, you can then unplug the power to physically remove power from the chassis if necessary.

Register the Firewall with the Management Center

Register the firewall with the management center depending on which deployment method you are using.

Add the Firewall to the Management Center Using Zero-Touch Provisioning

Zero-Touch Provisioning lets you register devices to the management center by serial number without having to perform any initial setup on the device. The management center integrates with the Cisco Security Cloud and CDO for this functionality.

When you use zero-touch provisioning, the following interfaces are preconfigured. Note that other settings, such as the DHCP server on inside, access control policy, or security zones, are not configured.

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration
- Ethernet 1/2 (or for the , the VLAN1 interface)— "inside", 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

High availability is only supported when you use the Management interface because zero-touch provisioning uses DHCP, which is not supported for data interfaces and high availability.

Note For management center version 7.4, you need to add the device using CDO; see the 7.4 guide for more information. The native management center workflow was added in 7.6. Also, for cloud integration in 7.4, see the **SecureX Integration** page in the management center.

Before you begin

- If the device does not have a public IP address or FQDN, set a public IP address/FQDN for the management center (for example, if it is behind NAT), so the device can initiate the management connection. See .

Procedure

Step 1 The first time you add a device using a serial number, integrate the management center with Cisco Security Cloud.

Note For a management center high-availability pair, you also need to integrate the secondary management center with Cisco Security Cloud.

a) Choose **Integration** > **Cisco Security Cloud**.
b) Click **Enable Cisco Security Cloud** to open a separate browser tab to log you into your Cisco Security Cloud account and confirm the displayed code.

Make sure this page is not blocked by a pop-up blocker. If you do not already have a Cisco Security Cloud and CDO account, you can add one during this procedure.

For detailed information about this integration, see .

CDO onboards the on-prem management center after you integrate the management center with Cisco Security Cloud. CDO needs the management center in its inventory for zero-touch provisioning to operate. However, you do not need to use CDO directly. If you do use CDO, its management center support is limited to device onboarding, viewing its managed devices, viewing objects associated with the management center, and cross-launching the management center.

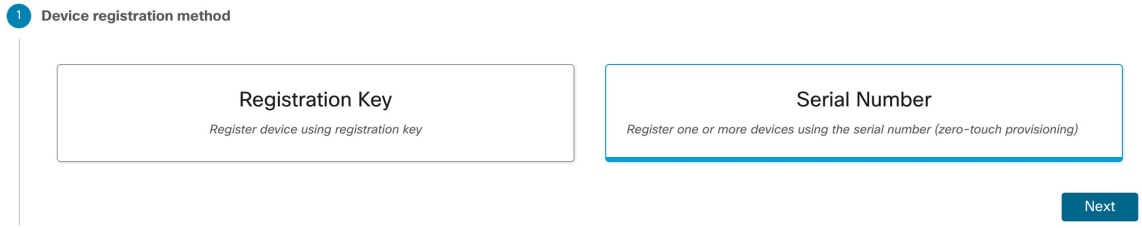
c) Make sure **Enable Zero-Touch Provisioning** is checked.
d) Click **Save**.

Step 2 Choose **Devices** > **Device Management**.

Step 3 From the **Add** drop-down menu, choose **Device (Wizard)**.

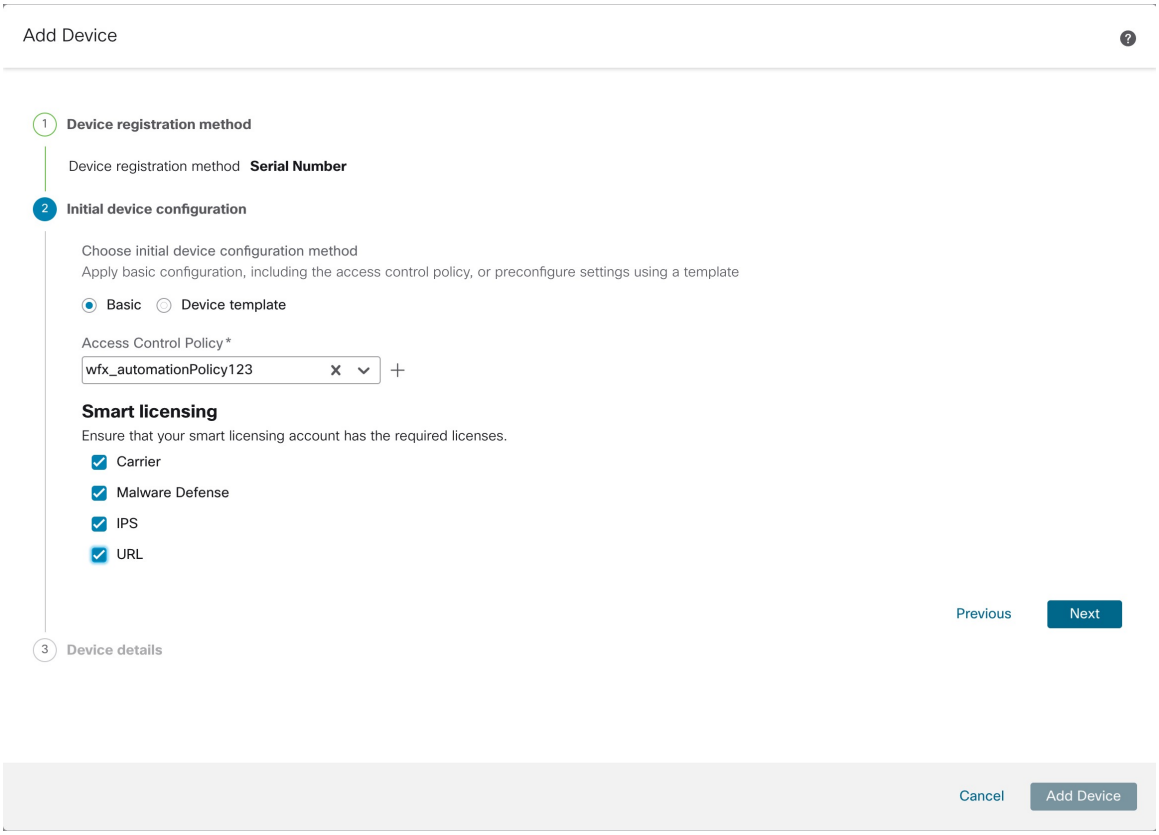
Step 4 Click **Use Serial Number**, and then click **Next**.

Figure 6: Device Registration Method



Step 5 For the **Initial device configuration**, click the **Basic** radio button.

Figure 7: Initial Device Configuration Method



a) Choose an initial **Access Control Policy** to deploy to the device upon registration, or create a new policy.

If the device is incompatible with the policy you choose, deploying will fail. This incompatibility could occur for multiple reasons, including licensing mismatches, model restrictions, passive vs inline issues, and other misconfigurations. After you resolve the issue that caused the failure, manually deploy configurations to the device.

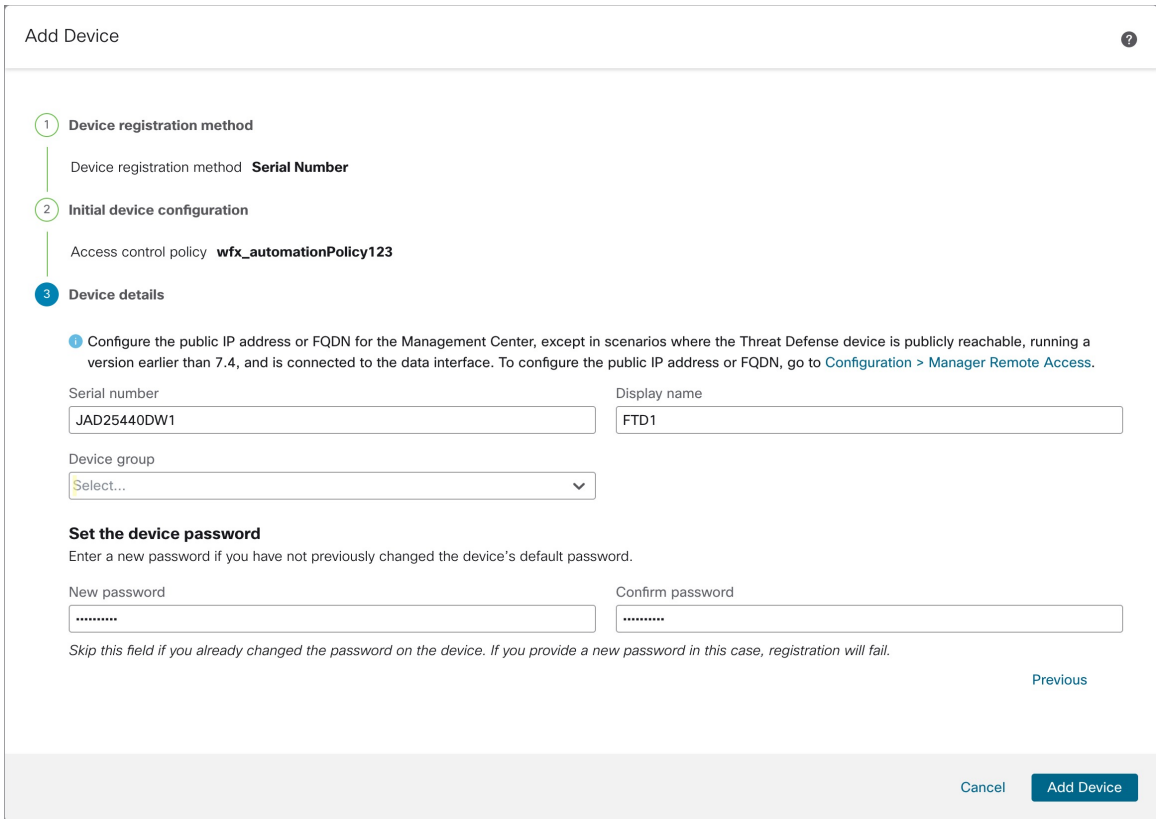
b) Choose **Smart licensing** licenses to apply to the device.

You can also apply licenses after you add the device, from the **System** > **Licenses** > **Smart Licenses** page.

c) Click **Next**.

Step 6 Configure the **Device details**.

Figure 8: Device details



a) Enter the **Serial number**.
b) Enter the **Display name** as you want it to display in the management center
c) (Optional) Choose the **Device Group**.
d) **Set the device password**.

   If this device is unconfigured or a fresh install, then you need to set a new password. If you already logged in and changed the password, then leave this field blank. Otherwise, registration will fail.

Step 7 Click **Add Device**.

It may take up to two minutes for the management center to verify the device's heartbeat and establish communication. If the registration succeeds, the device is added to the list.

Register the Firewall with the Management Center Using Manual Provisioning

Register the firewall to the management center.

Procedure

Step 1 Log into the management center.

a) Enter the following URL.

https://*fmc_ip_address*

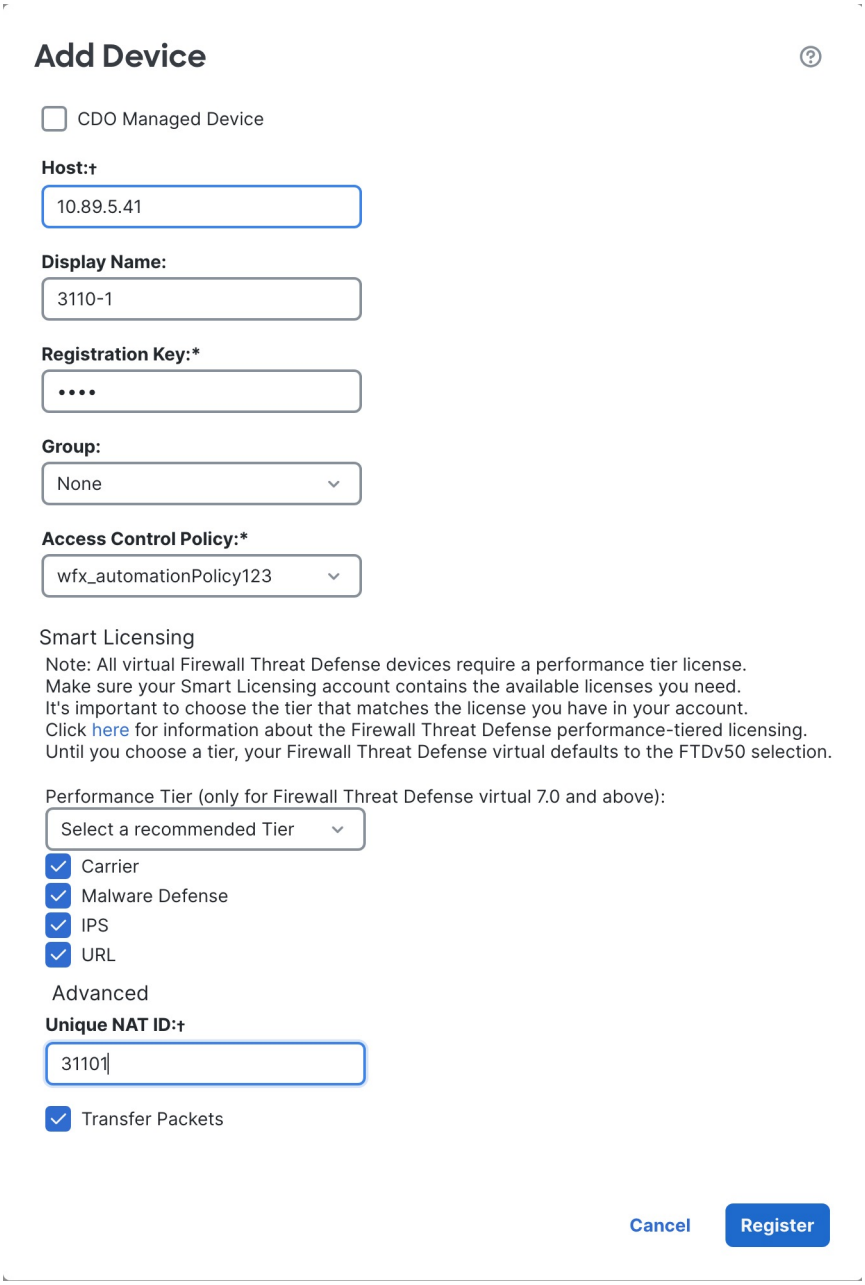
b) Enter your username and password.

c) Click **Log In**.

Step 2 Choose **Devices** > **Device Management**.

Step 3 From the **Add** drop-down list, choose **Add Device**.

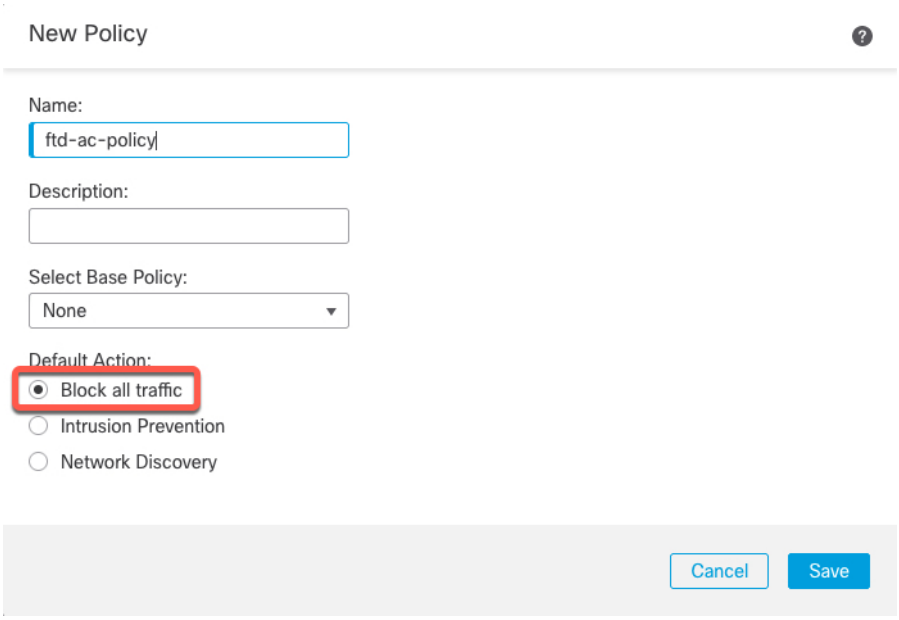
Figure 9: Add Device Using a Registration Key



Set the following parameters:

- **Host**—Enter the IP address or hostname of the firewall you want to add, if available. Leave this field blank if it is not available.
- **Display Name**—Enter the name for the firewall as you want it to display in the management center. You cannot change this name later.
- **Registration Key**—Enter the same registration key that you specified in the firewall initial configuration.
- **Domain**—Assign the device to a leaf domain if you have a multidomain environment.
- **Group**—Assign it to a device group if you are using groups.
- **Access Control Policy**—Choose an initial policy. Unless you already have a customized policy you know you need to use, choose **Create new policy**, and choose **Block all traffic**. You can change this later to allow traffic; see Configure an Access Control Rule.

Figure 10: New Policy



- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy. **Note:** You can apply the Secure Client remote access VPN license after you add the device, from the **System** > **Licenses** > **Smart Licenses** page.
- **Unique NAT ID**—Specify the NAT ID that you specified in the firewall initial configuration.
- **Transfer Packets**—Check the **Transfer Packets** check box so that for each intrusion event, the device transfers the packet to the management center for inspection.

  This option is enabled by default. For each intrusion event, the device sends event information and the packet that triggered the event to the management center for inspection. If you disable it, only event information will be sent to the management center; the packet will not be sent.

Step 4 Click **Register**.

If the threat defense fails to register, check the following items:

- Ping—Access the threat defense CLI (see Access the Threat Defense CLI), and ping the management center IP address using the following command:

  ping system *fmc_ip_address*

  If the ping is not successful, check your network settings using the **show network** command. If you need to change the firewall Management IP address, use the **configure network management-data-interface** command.

- Registration key, NAT ID, and the management center IP address—Make sure you are using the same registration key and NAT ID on both devices. You can set the registration key and NAT ID on the firewall using the **configure manager add** command.

For more troubleshooting information, see https://cisco.com/go/fmc-reg-error.