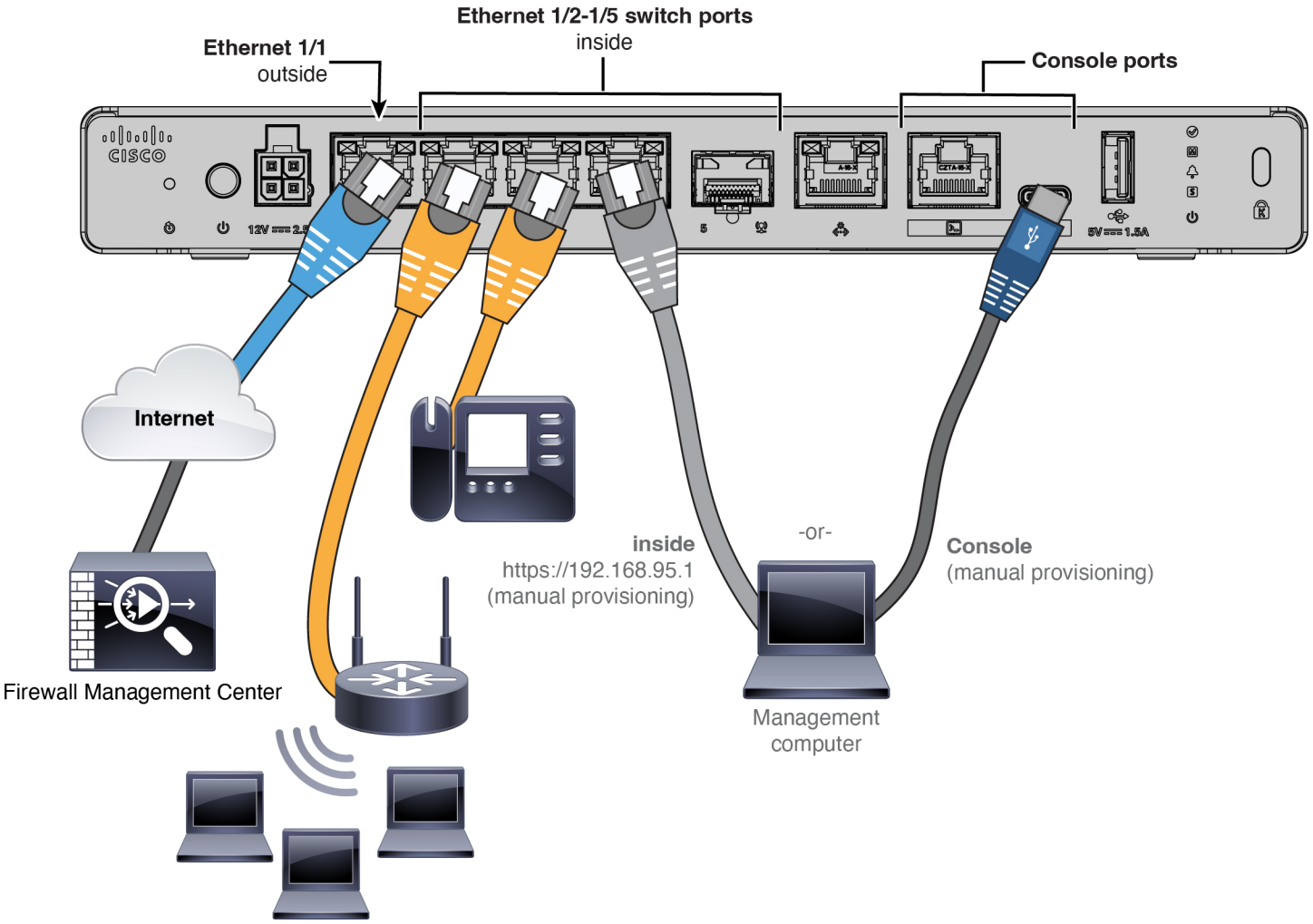
Cable and Register the Firewall

Cable the firewall and then register the firewall to the Firewall Management Center.

Cable the firewall

- Install an SFP into Ethernet 1/5—It is a 1-Gbps SFP port that requires an SFP module.
- See the hardware installation guide for more information.
- If you use zero-touch provisioning, do not cable both the outside and the Management interface. This guide covers management on the outside interface, but you may want to use zero-touch provisioning on Management with high availability. If you use zero-touch provisioning on outside and want to use high availability, you will have to change the outside IP address to a static address after registration.



Perform initial configuration (manual provisioning only)

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

Initial configuration: Firewall 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 Firewall 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 Firewall Device Manager.

a) Go to https://192.168.95.1.

b) Log in with the username **admin** and the default password **Admin123**.

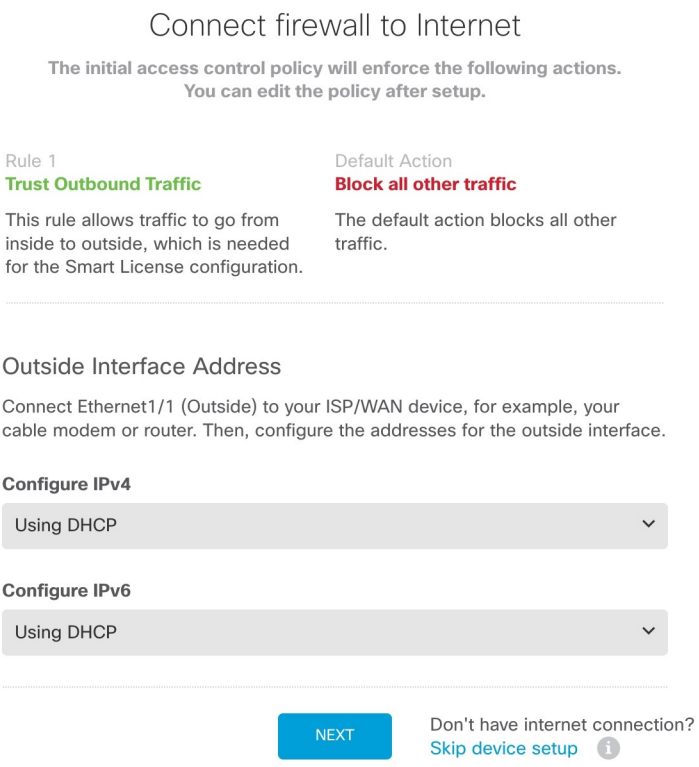
c) You are prompted to read and accept the General Terms and change the admin password.

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



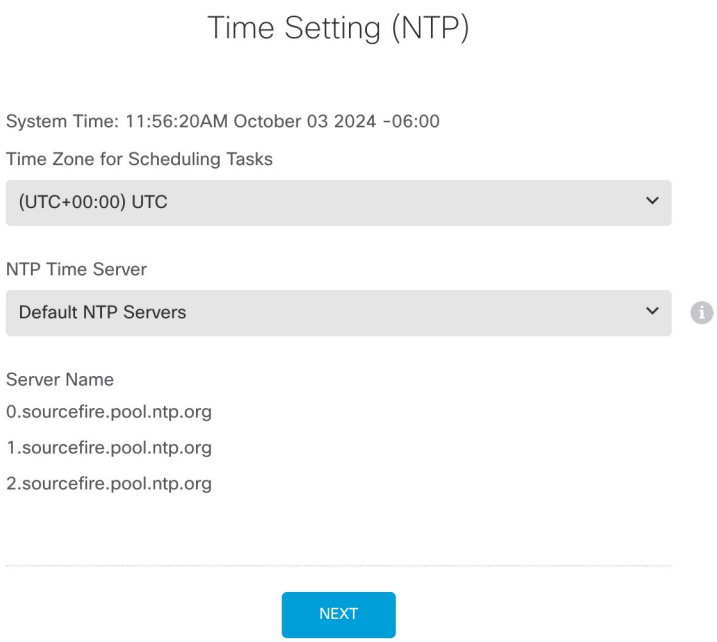
1. **Outside Interface Address**—Use a static IP address if you plan for high availability. You cannot configure PPPoE using the setup wizard; you can configure PPPoE after you complete the wizard.
2. **Management Interface**—The Management interface settings are used even though you are using manager 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.

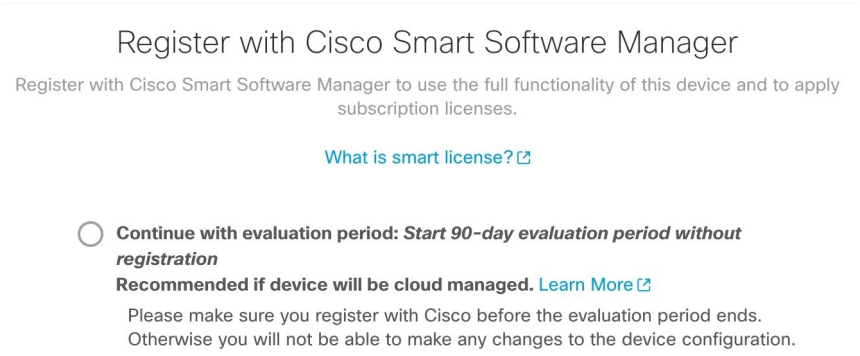
Firewall Hostname

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

Figure 2: Time Setting (NTP)



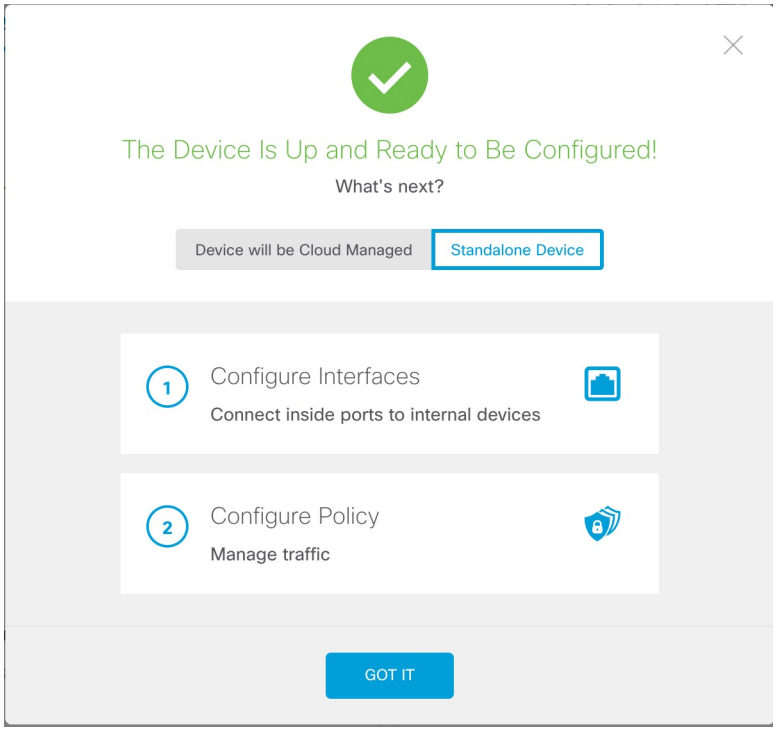
c) Select **Start 90 day evaluation period without registration**.



Do not register the Firewall Threat Defense with the Smart Software Manager; all licensing is performed on the Firewall Management CenterSecurity Cloud Control.

d) Click **Finish**.

Figure 3: What's Next



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

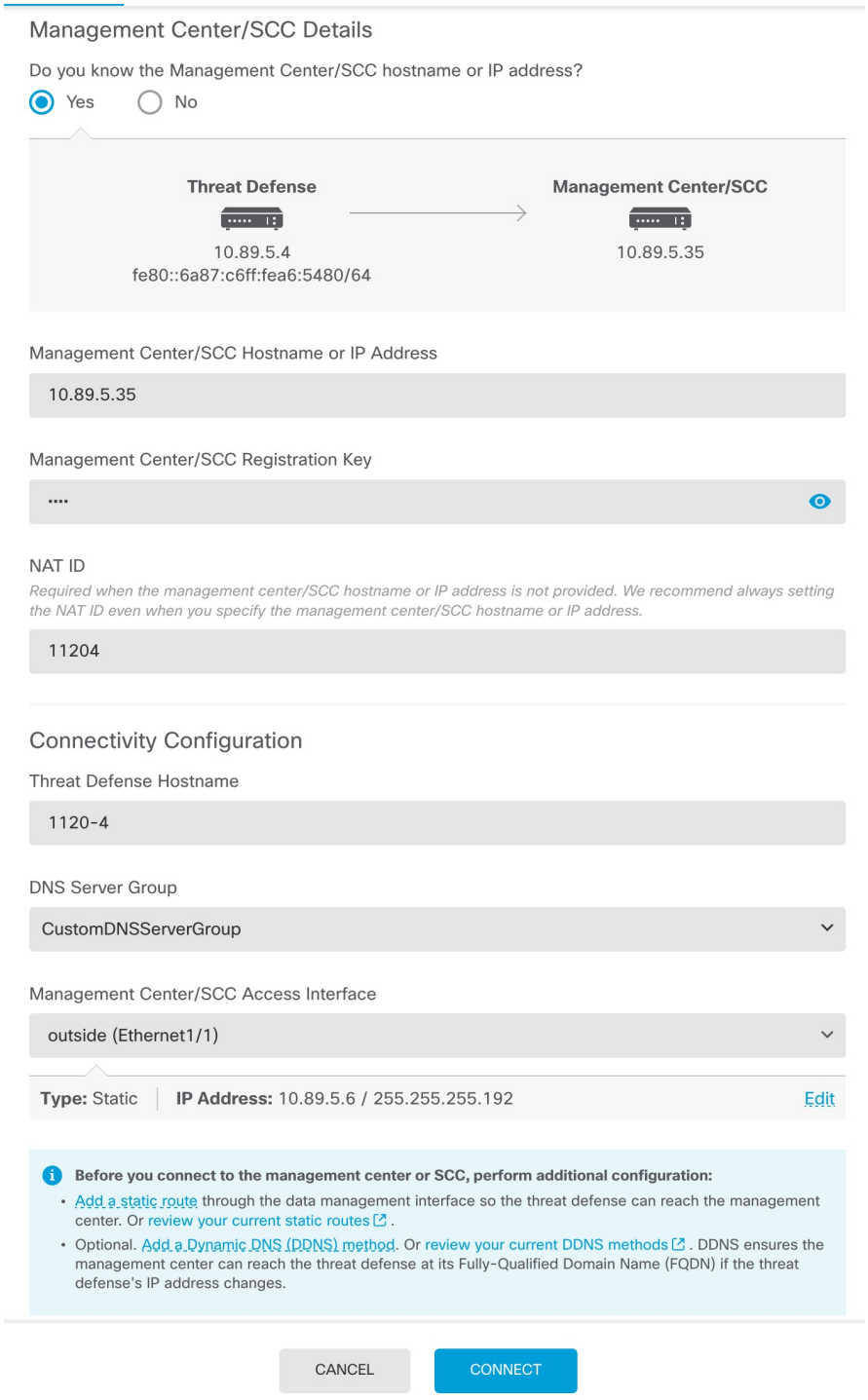
Step 4 If you want to configure additional interfaces, choose **Device**, and then click the link in the **Interfaces** summary.

Step 5 Register with the Firewall Management CenterSecurity Cloud Control by choosing **Device** > **System Settings** > **Central Management** and clicking **Proceed**

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

Note
Older versions may show "CDO" instead of "SCC."

Figure 4: Management Center/SCC Details



a) For **Do you know the Management Center/SCC Hostname or IP address**, click **Yes** if you can reach the Firewall Management Center using an IP address or hostname or **No** if the Firewall Management Center is behind NAT or does not have a public IP address or hostname.

b) If you chose **Yes**, enter the **Management Center/SCC Hostname/IP Address**.

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

This key is a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the firewall. The registration key must be between 2 and 36 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 Firewall 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 Firewall Management Center. We recommend that you specify the NAT ID even if you know the IP addresses of both devices. The NAT ID must be between 2 and 36 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 Firewall 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 Firewall Management Center.

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

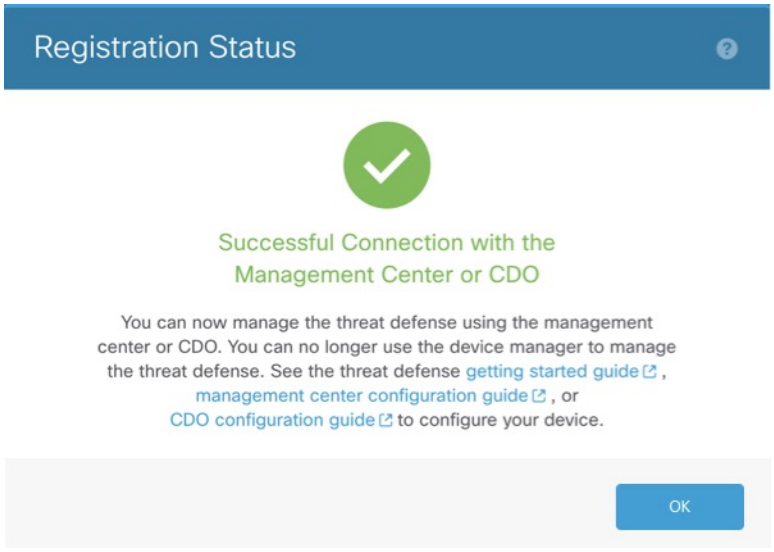
Step 7 (Optional) Click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the Firewall Management Center can reach the Firewall Threat Defense at its FQDN if the Firewall Threat Defense's IP address changes.

Step 8 Click **Connect**.

The **Registration Status** dialog box shows the current status of the Firewall Management CenterSecurity Cloud Control registration.

Figure 5: Successful Connection



Step 9 After the **Saving Management Center/SCC Registration Settings** step on the status screen, go to the Firewall Management CenterSecurity Cloud Control and add the firewall. See Add a firewall using manual provisioning, on page 17.

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 Firewall Threat Defense CLI. See Access the Firewall 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'

Manage the device locally? (yes/no) [yes]: no
```

Guidance: Enter **no** to use the Firewall Management Center.

```
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

After you press **Enter**, you are 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 Firewall 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 Firewall 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 Firewall Management Center. If the Firewall 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 Firewall Management Center when you register the Firewall Threat Defense. The registration key must be between 2 and 36 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 Firewall Management Center. The NAT ID must be between 2 and 36 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 Firewall Management Center.

Example:

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

Step 5 Shut down the Firewall 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 Firewall Management Center

Register the firewall with the Firewall Management Center depending on which deployment method you are using.

Add a firewall using the serial number (zero-touch provisioning)

Zero-Touch Provisioning lets you register devices to the Firewall Management Center by serial number without having to perform any initial setup on the device. The Firewall Management Center integrates with Security Cloud Control for this functionality.

Note For Firewall Management Center version 7.4, you need to add the device using Security Cloud Control; see the 7.4 guide for more information. The native Firewall Management Center workflow was added in 7.6. Also, for cloud integration in 7.4, see the **SecureX Integration** page in the Firewall Management Center.

Default Configuration After Registration

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 200, the VLAN1 interface)— "inside", 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

Requirements

When you use the outside interface for manager access, it uses DHCP by default. Before you can enable high availability, you need to change the IP address to a static address. Alternatively, you can use the Management interface instead; DHCP is supported on Management with high availability.

Before you begin

- If the device does not have a public IP address or FQDN, set a public IP address/FQDN for the Firewall Management Center (for example, if it is behind NAT), so the device can initiate the management connection. See **Administration** > **Configuration** > **Manager Remote Access**.
- DHCP server for either Management or Ethernet 1/1 that provides an IP address and default gateway.
- Network access to the OpenDNS public DNS servers. IPv4: 208.67.220.220 and 208.67.222.222; IPv6: 2620:119:35::35. DNS servers obtained from DHCP are never used.

  The following names need to be resolved:

Table 1: FQDNs for zero-touch provisioning

FQDNs
*.cisco.com (many FQDNs)
*.defenseorchestrator.com (many FQDNs)
*.defenseorchestrator.eu (for the EU, many FQDNs)
0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org
1.200.159.162.in-addr.arpa
60.19.239.178.in-addr.arpa
connected.by.freedominter.net
time.cloudflare.com
udc.neo4j.org

Procedure

Step 1 The first time you add a device using a serial number, integrate the Firewall Management Center with Security Cloud Control.

Note
For a Firewall Management Center high-availability pair, you also need to integrate the secondary Firewall Management Center with Security Cloud Control.

a) Choose **Integrations** > **Security Cloud Control**.
b) Click **Enable Security Cloud Control** to open a separate browser tab to log you into your Security Cloud Control 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 Security Cloud Control account, you can add one during this procedure.

For detailed information about this integration, see the "System Configuration" chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

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

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

Step 2 Obtain your device's serial number.

The device includes two serial numbers: the chassis serial number and the PCB (circuit board) serial number. Either serial number should work.

- If you have the shipping box, you can see the chassis serial number on the label.
- The chassis serial number is on the compliance label on .
- The PCB serial number is on a label on the chassis called "S/N."
- You can view the serial numbers using the following CLI commands:
  - FXOS—**show chassis detail** shows both serial numbers.
  - Firewall Threat Defense—**show inventory** shows the chassis serial number. **show serial-number** shows the PCB serial number.

Step 3 Check your LEDs to make sure the firewall is ready for registration.

Table 2: Zero-Touch Provisioning: Managed (M) LED behavior

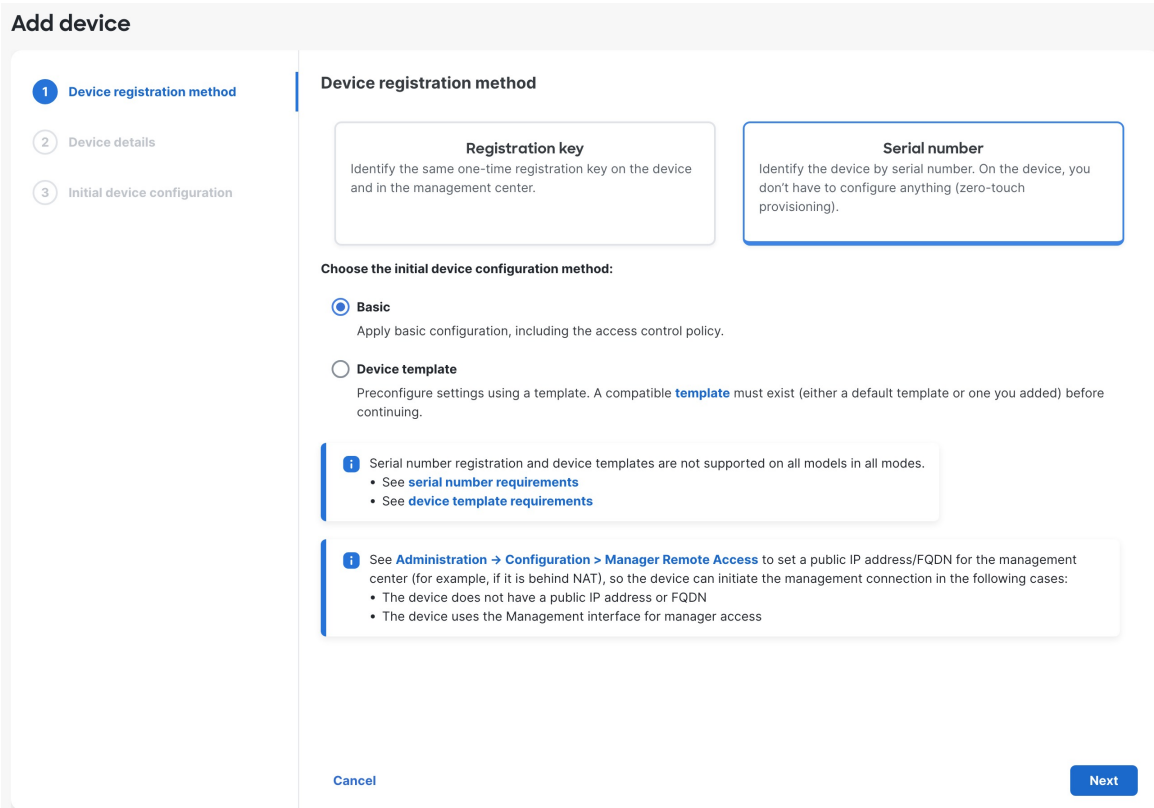
M LED	Description	Time after firewall powered on (minutes:seconds)
Slow flashing green	Connected to the Cisco cloud and ready for onboarding	15:00 - 30:00
Alternating green and amber (error condition)	Failed to connect to the Cisco cloud	15:00 - 30:00
Solid green	Onboarded	20:00 - 45:00

Step 4 Choose **Devices** > **Device Management**.

Step 5 From the **Add** drop-down menu, choose **Device**.

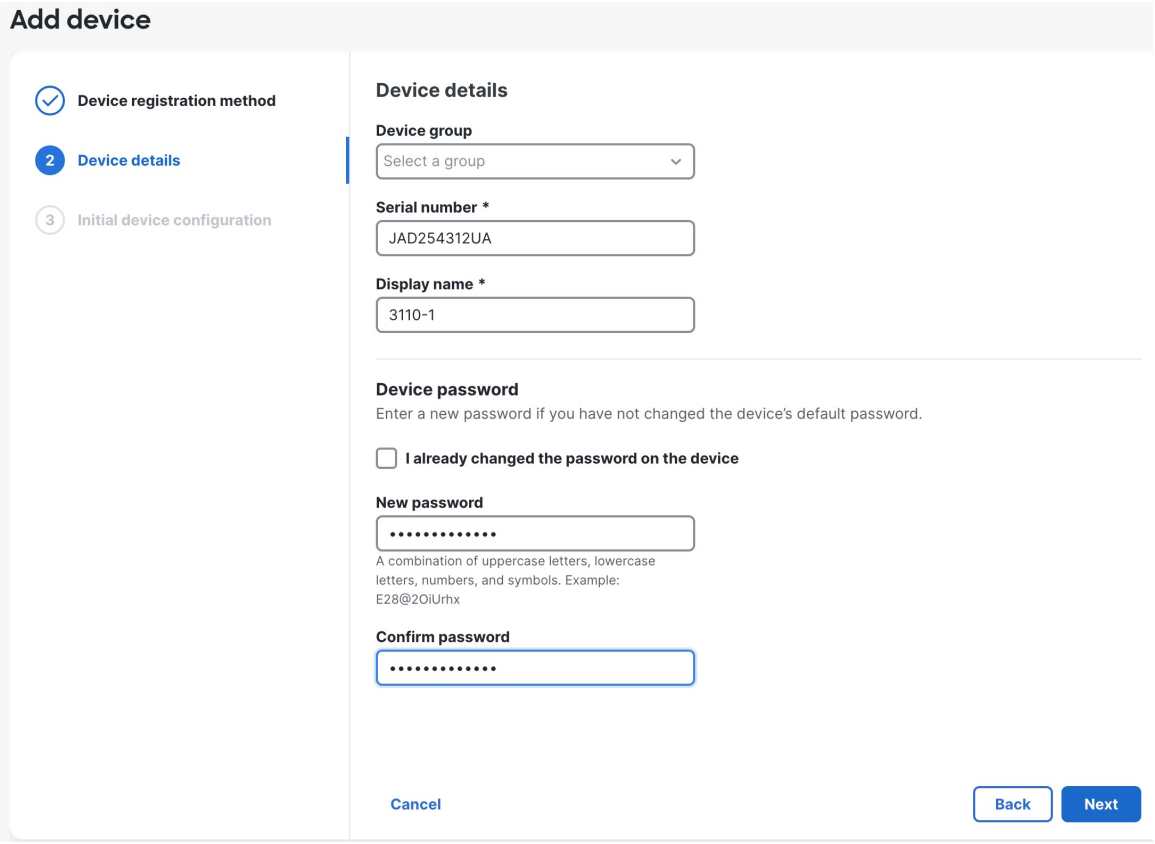
Step 6 Click **Serial Number**, click **Basic**, and then click **Next**.

Figure 6: Device Registration Method



Step 7 Configure the device details and click **Next**.

Figure 7: Device Details

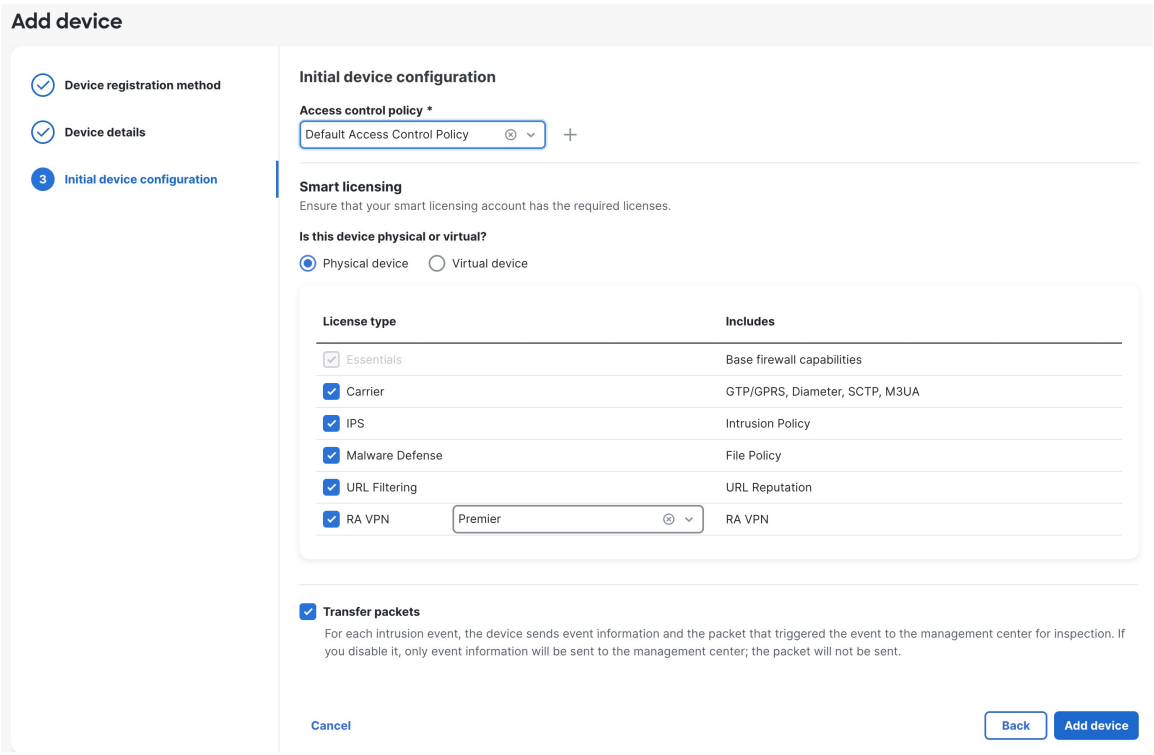


- **Domain**—In a multidomain environment, choose the leaf domain.
- **Device group**—In a single domain environment, add the device to a **Device group**.
- **Serial number**—Enter the IP address or the hostname of the device you want to add. Leave this field blank if you don't know the device IP address (for example, it's behind NAT).
- **Display name**—Enter a name for the device as you want it to display in the Firewall Management Center. You cannot change this name later.
- **Device password**—If this device is unconfigured or a fresh install, then you need to set a **New Password** and confirm the password.

  Check **I already changed the password on the device** only if you already logged in and changed the password. Otherwise, registration will fail.

Step 8 Configure the initial device configuration.

Figure 8: Initial Device Configuration



- **Access control policy**—Choose an initial policy to deploy to the device at registration, or create a new policy. Unless you already have a customized policy you know you need to use, choose **Add** (+), and choose **Block all traffic**. You can change this later to allow traffic.
- **Smart licensing**—Choose your licenses.
  - **Is this device physical or virtual?**—Choose **Physical device**
  - **License type**—Check each license type to assign to the device.

  You can also apply licenses after you add the device.
- **Transfer packets**—Enable this option so that for each intrusion event, the device transfers the packet to the Firewall Management Center for inspection.

  For each intrusion event, the device sends event information and the packet that triggered the event to the Firewall Management Center for inspection. If you disable it, only event information will be sent to the Firewall Management Center; the packet will not be sent.

Step 9 Click **Add device**.

It may take up to two minutes for the Firewall Management Center to verify the device's heartbeat and establish communication.

When using zero-touch provisioning on the outside interface, Security Cloud Control acts as a DDNS provider and does the following:

- Enables DDNS on outside using the **FMC Only** method. This method is only supported for zero-touch provisioning devices.
- Maps the outside IP address with the following hostname: *serial-number*.**local**.
- Provides the IP address/hostname mapping to the Firewall Management Center so it can resolve the hostname to the correct IP address.
- Informs the Firewall Management Center if the IP address ever changes, for example, if the DHCP lease renews.

If you use zero-touch provisioning on the Management interface, DDNS is not supported. The Firewall Management Center must be publicly reachable so the device can initiate the management connection.

You can continue to use Security Cloud Control as the DDNS provider, or you can later change the DDNS configuration in the Firewall Management Center to a different method.

Add a firewall using manual provisioning

Register the firewall to the Firewall Management Center manually using the device IP address or hostname and a registration key.

Procedure

Step 1 Log into the Firewall Management Center.

a) Enter the following URL.

https://*fmc_ip_address*

b) Enter your username and password.

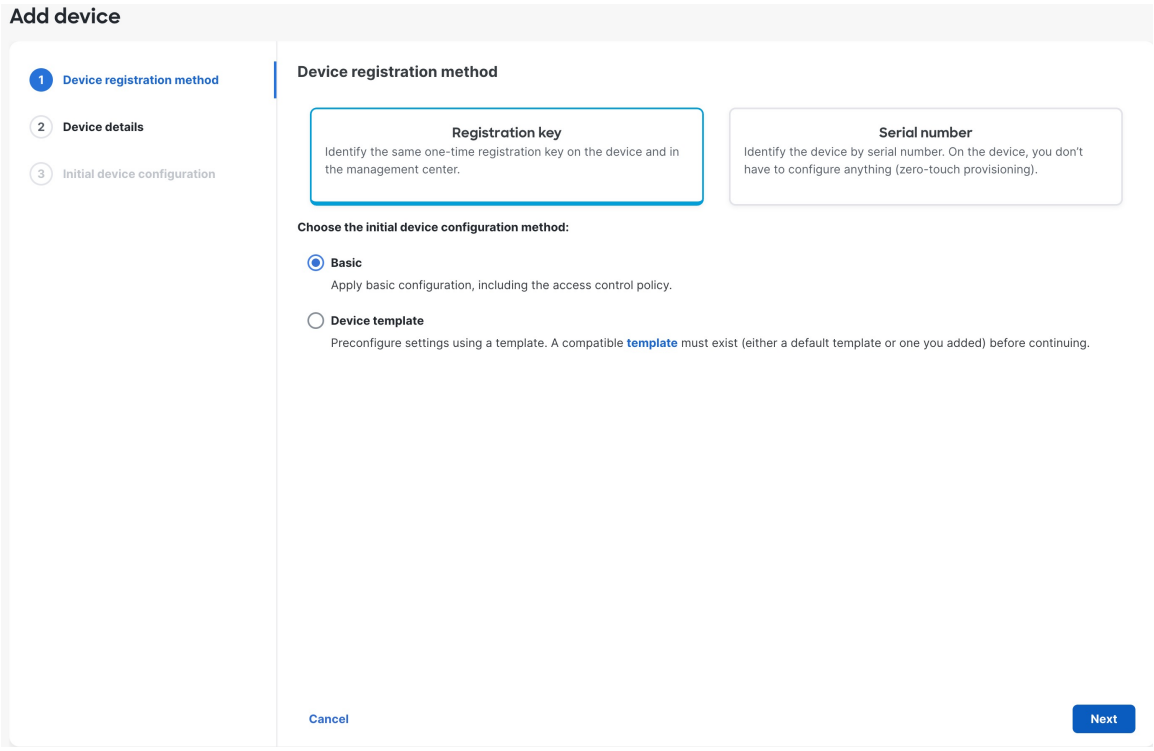
c) Click **Log In**.

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

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

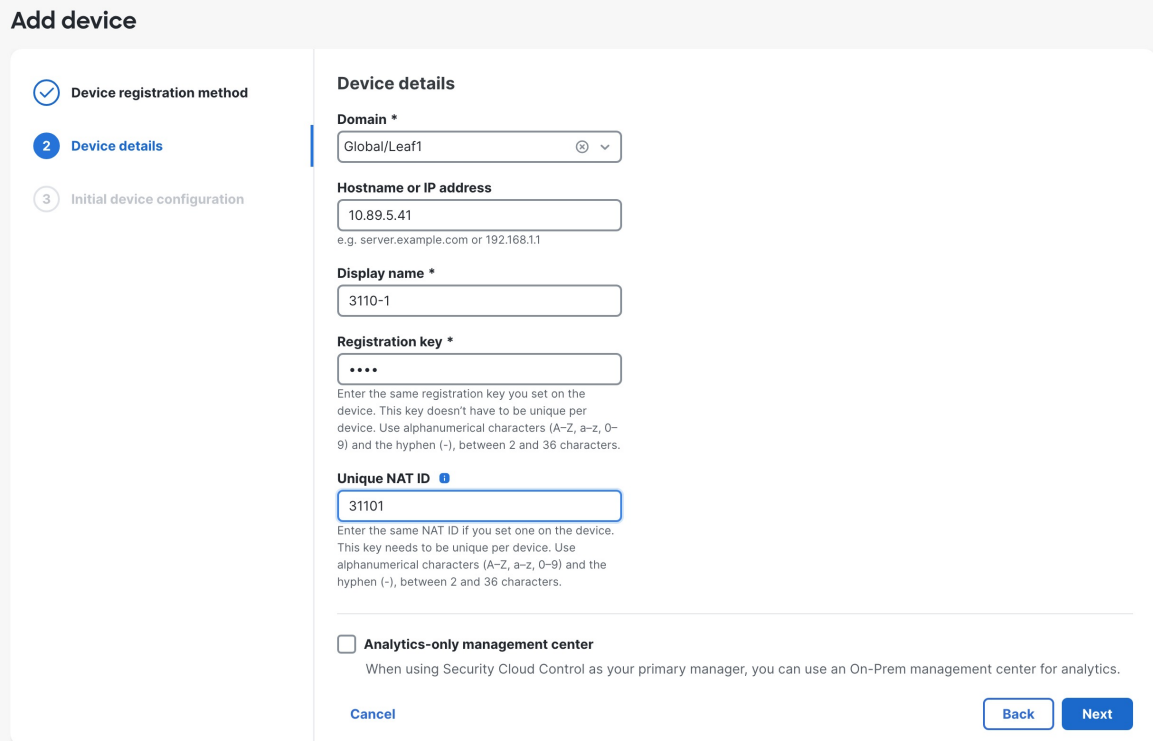
Step 4 Click **Registration Key**, click **Basic**, and then click **Next**.

Figure 9: Device Registration Method



Step 5 Configure the device details and click **Next**.

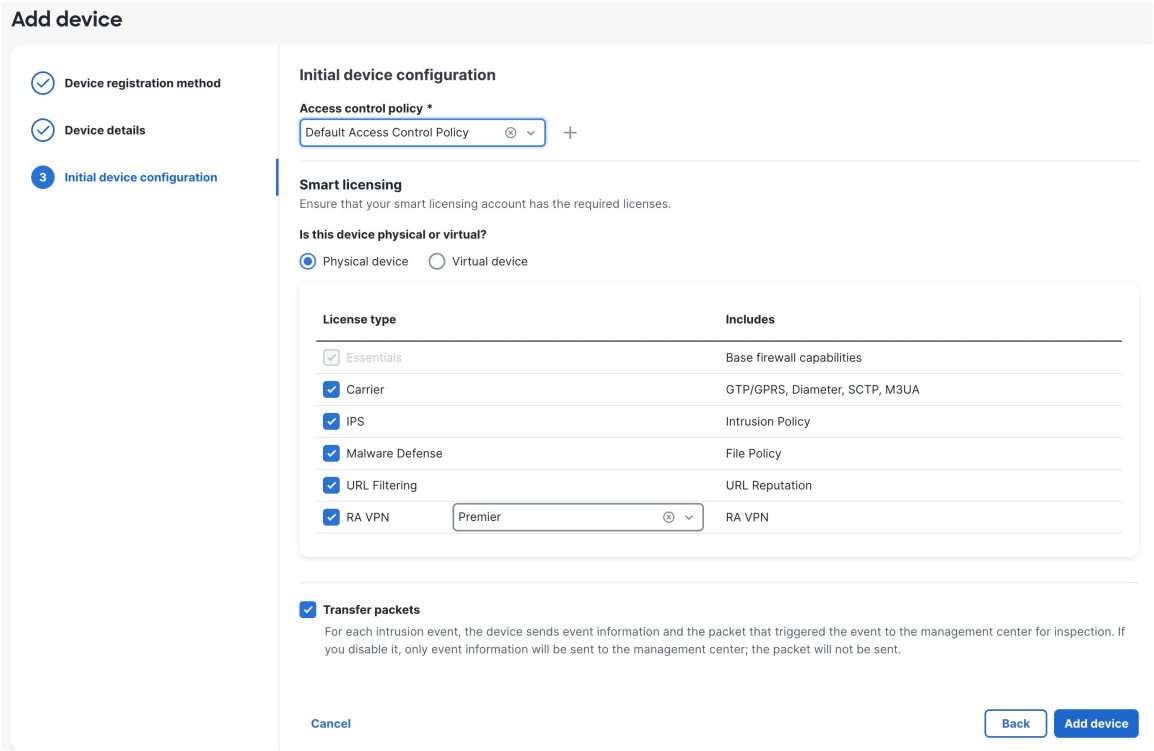
Figure 10: Device Details



- **Domain**—In a multidomain environment, choose the leaf domain.
- **Device group**—In a single domain environment, add the device to a **Device group**.
- **Hostname or IP address**—Enter the IP address or the hostname of the device you want to add. Leave this field blank if you don't know the device IP address (for example, it's behind NAT).
- **Display name**—Enter a name for the device as you want it to display in the Firewall Management Center. You cannot change this name later.
- **Registration key**—Enter the same registration key from your initial configuration.
- **Unique NAT ID**—Enter the same ID from your initial configuration.
- **Analytics-only management center**—Leave this unchecked.

Step 6 Configure the initial device configuration.

Figure 11: Initial Device Configuration



- **Access control policy**—Choose an initial policy to deploy to the device at registration, or create a new policy. Unless you already have a customized policy you know you need to use, choose **Add** (+), and choose **Block all traffic**. You can change this later to allow traffic.
- **Smart licensing**—Choose your licenses.
  - **Is this device physical or virtual?**—Choose **Physical device**
  - **License type**—Check each license type to assign to the device.

  You can also apply licenses after you add the device.
- **Transfer packets**—Enable this option so that for each intrusion event, the device transfers the packet to the Firewall Management Center for inspection.

  For each intrusion event, the device sends event information and the packet that triggered the event to the Firewall Management Center for inspection. If you disable it, only event information will be sent to the Firewall Management Center; the packet will not be sent.

Step 7 Click **Add device**.

It may take up to two minutes for the Firewall Management Center to verify the device's heartbeat and establish communication. If the registration succeeds, the device is added to the list. If it fails, you will see an error message. If the device fails to register, check the following items:

- Ping—Access the device CLI, and ping the Firewall Management Center IP address using the following command:

  ping system *ip_address*

If the ping is not successful, check your network settings using the **show network** command. If you need to change the device IP address, use the **configure network** {**ipv4** | **ipv6**} **manual** command.

- Registration key, NAT ID, and Firewall Management Center IP address—Make sure you are using the same registration key, and if used, NAT ID, on both devices. You can set the registration key and NAT ID on the device using the **configure manager add** command.

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