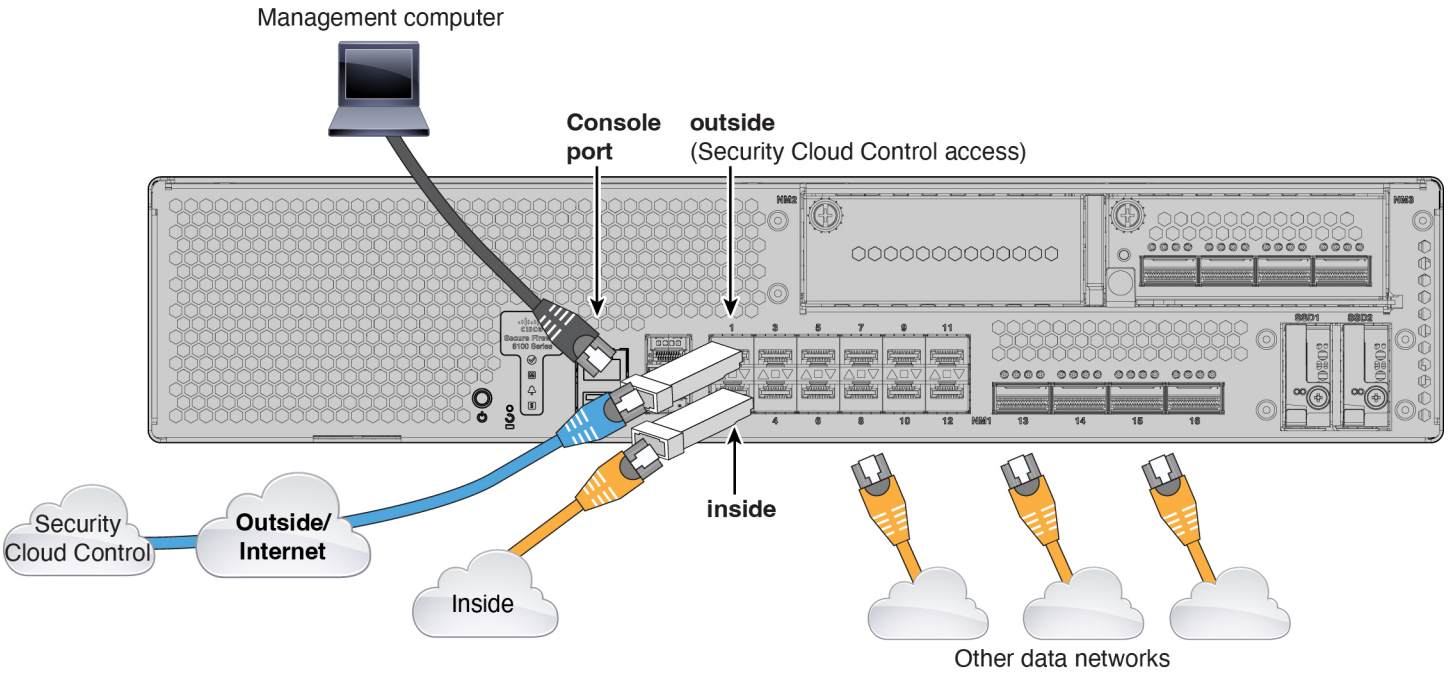
Cable and Onboard the Firewall

Cable and onboard the firewall to Security Cloud Control.

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—Ethernet 1/1 to 1/12 fixed ports are 1/10/25/50-Gbps SFP28 ports that require SFP/SFP+/SFP28 modules; Ethernet 1/13 through 1/16 are 1/10/25/50-Gbps QSFP28 ports that require SFP/SFP+/QSFP+/SFP28/QSFP28 modules.
- See the hardware installation guide for more information.



Onboard the firewall

Onboard the firewall using a CLI registration key.

Procedure

Step 1 In the Security Cloud Control navigation menu, click **Security Devices**, then click the blue plus button ( ) to **Onboard** a device.

Step 2 Click the **FTD** tile.

Step 3 Under **Management Mode**, be sure **FTD** is selected.

Step 4 Select **Use CLI Registration Key** as the onboarding method.

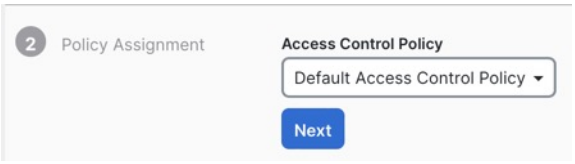
Figure 1: Use CLI Registration Key

Step 5 Enter the **Device Name** and click **Next**.

Figure 2: Device Name

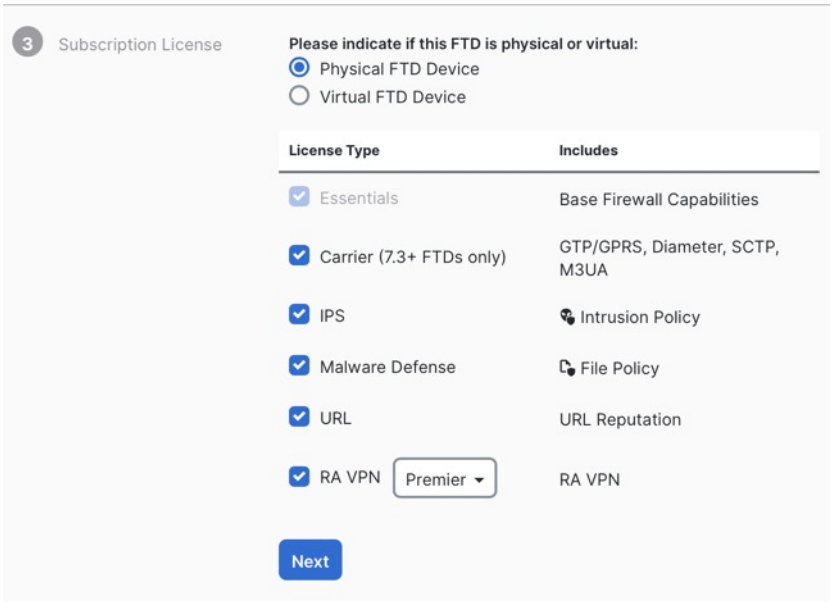
Step 6 For the **Policy Assignment**, use the drop-down menu to choose an access control policy for the device. If you have no policies configured, choose the **Default Access Control Policy**.

Figure 3: Access Control Policy



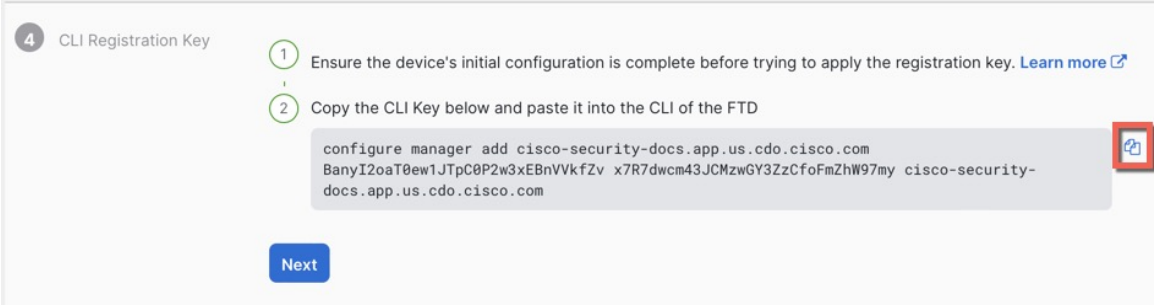
Step 7 For the **Subscription License**, click the **Physical FTD Device** radio button, and then check each of the feature licenses you want to enable. Click **Next**.

Figure 4: Subscription License



Step 8 For the **CLI Registration Key**, Security Cloud Control generates a command with the registration key and other parameters. You must copy this command and use it in the intial configuration of the Firewall Threat Defense.

Figure 5: CLI Registration Key



configure manager add Security Cloud Control_*hostname registration_key nat_id display_name*

Copy this command at the Firewall Threat Defense CLI after you complete the startup script. See Perform initial configuration, on page 4.

Example:

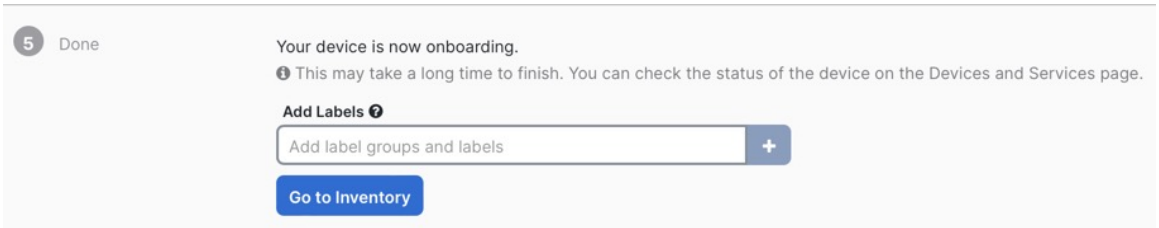
Sample command for CLI setup:

```
configure manager add account1.app.us.scc.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.scc.cisco.com
```

Step 9 Click **Next** in the onboarding wizard to start registering the device.

Step 10 (Optional) Add labels to your device to help sort and filter the **Security Devices** page. Enter a label and select the blue plus button (+). Labels are applied to the device after it's onboarded to Security Cloud Control.

Figure 6: Done



Perform initial configuration

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'
```

```
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 Security Cloud Control that will manage this Firewall Threat Defense using the **configure manager add** command that Security Cloud Control generated. See Onboard the firewall, on page 2 to generate the command.

Example:

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
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.