# Firepower 1010 Threat Defense Getting Started: Device Manager

**First Published:** 2024-10-16

**Last Modified:** 2024-10-21

**C H A P T E R 1**

# Before You Begin

Manage a firewall using the local Secure Firewall device manager.

# Cable the Firewall

See the hardware installation guide for more information.



**Ethernet 1/2-1/8 Switch Ports**
inside, 192.168.95.1
PoE+ on Ethernet 1/7 and 1/8

**Ethernet 1/1**
outside, DHCP and IPv6 autoconfig
from Modem

(Alternative) **Management 1/1**
management,
DHCP from management nw

Internet

Modem or Router

Management Computer
DHCP from inside: 192.168.95.x

(Optional)
**Console ports**
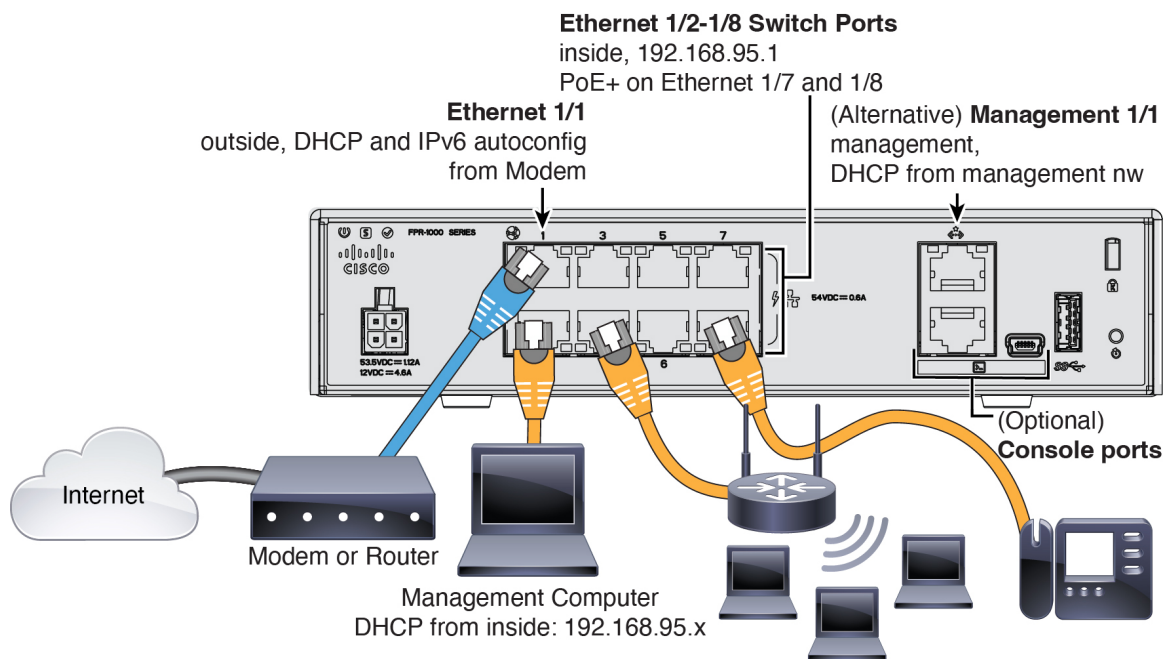
# Power On the Firewall

System power is controlled by the power cord; there is no power button.

✎

**Note**     The first time you boot up the firewall, threat defense initialization can take approximately 15 to 30 minutes.

### Before you begin

It's important that you provide reliable power for your firewall (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.
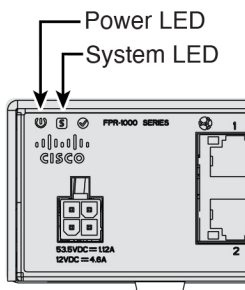
**Procedure**

**Step 1**     Attach the power cord to the firewall, and connect it to an electrical outlet.

The power turns on automatically when you plug in the power cord.

**Step 2**     Check the Power LED on the back of the firewall; if it is solid green, the firewall is powered on.

*Figure 1: System and Power LEDs*



**Step 3**     Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.
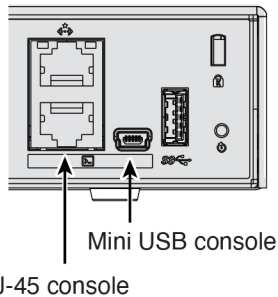
# Which Application is Installed: Threat Defense or ASA?

Both applications, threat defense or ASA, are supported on the hardware. Connect to the console port and determine which application was installed at the factory.

**Procedure**

**Step 1**  Connect to the console port using either port type.

**Figure 2: Console Port**



Mini USB console

RJ-45 console

**Step 2**  See the CLI prompts to determine if your firewall is running threat defense or ASA.

**Threat Defense**

You see the firepower login (FXOS) prompt. You can disconnect without logging in and setting a new password. If you need to log in all the way, see Access the Threat Defense CLI, on page 3.

```
firepower login:
```

**ASA**

You see the ASA prompt.

```
ciscoasa>
```

**Step 3**  If you are running the wrong application, see Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.
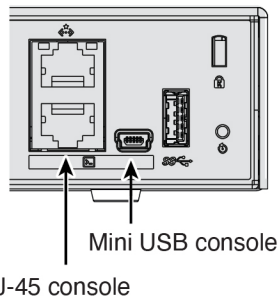
# Access the Threat Defense CLI

You might need to access the CLI for configuration or troubleshooting.

**Procedure**

**Step 1**  Connect to the console port using either port type.

*Figure 3: Console Port*

Mini USB console

RJ-45 console

**Step 2**    You connect to FXOS. Log in to the CLI using the **admin** username and the password (the default is **Admin123**). The first time you log in, you are prompted to change the password.

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

**Step 3**    Change to the threat defense CLI.

**Note**    If you want to use the device manager for initial setup, do not access the threat defense CLI, which starts the CLI setup.

**connect ftd**

The first time you connect to the threat defense CLI, you are prompted to complete initial setup.

**Example:**

```
firepower# connect ftd
>
```

To exit the threat defense CLI, enter the **exit** or **logout** command. This command returns you to the FXOS prompt.

**Example:**

```
> exit
firepower#
```

# Check the Version and Reimage

We recommend that you install your target version before you configure the firewall. Alternatively, you can perform an upgrade after you are up and running, but upgrading, which preserves your configuration, may take longer than using this procedure.
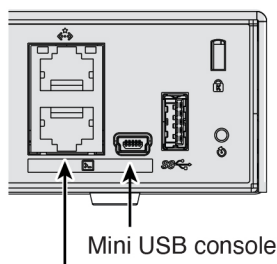
**What Version Should I Run?**

Cisco recommends running a Gold Star release indicated by a gold star next to the release number on the software download page. You can also refer to the release strategy described in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html.

**Procedure**

**Step 1**    Connect to the console port using either port type.

**Figure 4: Console Port**



Mini USB console

RJ-45 console

**Step 2**    At the FXOS CLI, show the running version.

**scope ssa**

**show app-instance**

**Example:**

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name Slot ID Admin State Operational State Running Version Startup Version Cluster Oper
 State
---------------- ------- ----------- ----------------- --------------- ---------------
------------------
ftd              1       Enabled     Online            7.6.0.65        7.6.0.65        Not Applicable
```

**Step 3**    If you want to install a new version, perform these steps.

   a)   By default, the Management interface uses DHCP. If you need to set a static IP address for the Management interface, enter the following commands.

        **scope fabric-interconnect a**

**set out-of-band static ip** *ip* **netmask** *netmask* **gw** *gateway*

**commit-buffer**

| Note | If you encounter the following error, you must disable DHCP before committing the change. Follow the commands below to disable DHCP. |
|------|--------|

```
firepower /fabric-interconnect* # commit-buffer
Error: Update failed: [Management ipv4 address (IP <ip> / net mask <netmask> ) is not
in the same network of current DHCP server IP range <ip - ip>.
Either disable DHCP server first or config with a different ipv4 address.]
firepower /fabric-interconnect* # exit
firepower* # scope system
firepower /system* # scope services
firepower /system/services* # disable dhcp-server
firepower /system/services* # commit-buffer
```

b) Perform the reimage procedure in the FXOS troubleshooting guide.

You will need to download the new image from a server accessible from the Management interface.

After the firewall reboots, you connect to the FXOS CLI again.

c) At the FXOS CLI, you are prompted to set the admin password again.

# (Optional) Change Management Network Settings at the CLI

By default, you can manage the firewall on either of the following interfaces:

- Ethernet 1/2 through Ethernet 1/8—192.168.95.1/24
- Management 1/1—IP address from DHCP

If you cannot use the default IP addresses, then you can connect to the console port and perform initial setup at the CLI to set the Management 1/1 IP address to a static address.

**Procedure**

**Step 1**    Connect to the console port. See Which Application is Installed: Threat Defense or ASA?, on page 2.

**Step 2**    Connect to the threat defense CLI.

**connect ftd**

**Example:**

```
firepower# connect ftd
>
```

**Step 3**    Complete the CLI setup script for the Management interface settings.

```
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.

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

**Guidance:** Choose **manual** to set a static IP address.

```
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]: 10.10.10.1
```

**Guidance:** Set an IP address for the gateway.

```
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

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]: yes

>
```

**Guidance:** Enter **yes** to use the device manager.

**Step 4**     Log into the device manager on the new Management IP address.

# Obtain Licenses

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. If you don't have an account on the Smart Software Manager, click the link to set up a new account.

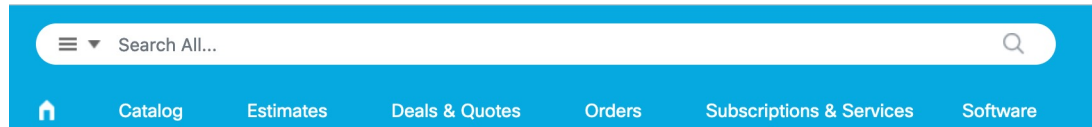The threat defense has the following licenses:

- Essentials—Required

&bull; IPS

&bull; Malware Defense

&bull; URL Filtering

&bull; Cisco Secure Client

1.  If you need to add licenses yourself, go to Cisco Commerce Workspace and use the **Search All** field.

    **Figure 5: License Search**

    

2.  Search for the following license PIDs.

    ✎

    **Note**   If a PID is not found, you can add the PID manually to your order.

    &bull; IPS, Malware Defense, and URL combination:

    &bull; L-FPR1010T-TMC=

    When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:

    &bull; L-FPR1010T-TMC-1Y

    &bull; L-FPR1010T-TMC-3Y

    &bull; L-FPR1010T-TMC-5Y

    &bull; Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

3.  Choose **Products & Services** from the results.

    **Figure 6: Results**
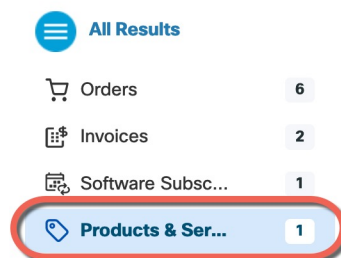
# (If Needed) Power Off the Firewall

It's important that you shut down your system properly. Simply unplugging the power can cause serious file system damage. 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 firewall system.

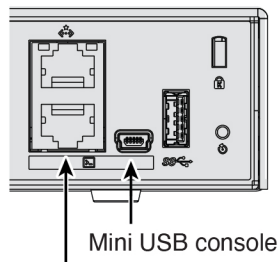The Firepower 1010 chassis does not have an external power switch..

## Power Off the Firewall at the CLI

You can use the FXOS CLI to safely shut down the system and power off the firewall.

**Procedure**

**Step 1**    Connect to the console port using either port type.

**Figure 7: Console Port**



Mini USB console

RJ-45 console

**Step 2**    In the FXOS CLI, connect to local-mgmt mode.

firepower # **connect local-mgmt**

**Step 3**    Shut down the system.

firepower(local-mgmt) # **shutdown**

**Example:**

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.   Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

**Step 4**    Monitor the system prompts as the firewall shuts down. When the shutdown is complete, you will see the following prompt.

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

**Step 5**     You can now unplug the power to physically remove power from the chassis if necessary.

# Power Off the Firewall Using the Device Manager

Shut down your system properly using the device manager.

**Procedure**

**Step 1**     Shut down the firewall.

a)   Click **Device**, then click the **System Settings** > **Reboot/Shutdown** link.

b)   Click **Shut Down**.

**Step 2**     If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. When shutdown is complete, you will see the following prompt.

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

**Step 3**     You can now unplug the power to physically remove power from the chassis if necessary.

**CHAPTER 2**

# Configure a Basic Policy

Complete the initial configuration and then configure additional interfaces and network settings as well as customizing your policy.

## Log Into the Device Manager

Log into the device manager to configure your threat defense.

**Procedure**

**Step 1** Enter the following URL in your browser, depending on which interface your computer is connected to.

- Ethernet 1/2 through Ethernet 1/8—**https://192.168.95.1**

- Management 1/1—**https://**_management_ip_ (from DHCP)

**Step 2** Log in with the username **admin**, and the default password **Admin123**.

## Complete the Initial Configuration

Use the setup wizard when you first log into the device manager to complete the initial configuration. After you complete the setup wizard, you should have a functioning device with a couple of basic policies in place:
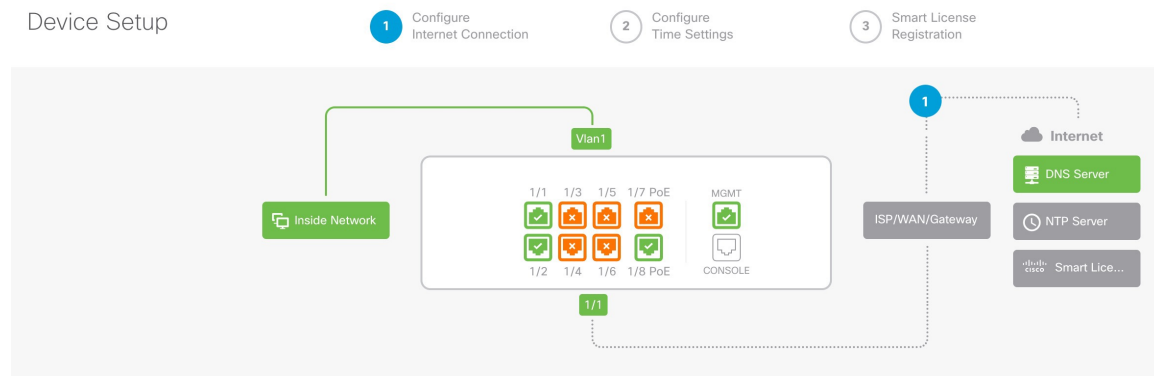
- inside→outside traffic flow

- Interface PAT for all traffic to outside.

**Procedure**

**Step 1**    Accept the General Terms and change the admin password.

The **Device Setup** screen appears.

**Figure 8: Device Setup**



**Note**                         The exact port configuration depends on your model.

**Step 2**    Configure network settings for the outside and management interfaces.

***Figure 9: Connect firewall to internet***

## Connect firewall to Internet

The initial access control policy will enforce the following actions.
You can edit the policy after setup.

Rule 1
**Trust Outbound Traffic**

This rule allows traffic to go from
inside to outside, which is needed
for the Smart License configuration.

Default Action
**Block all other traffic**

The default action blocks all other
traffic.

### Outside Interface Address

Connect Ethernet1/1 (Outside) to your ISP/WAN device, for example, your
cable modem or router. Then, configure the addresses for the outside interface.

**Configure IPv4**

| Using DHCP | ∨ |

**Configure IPv6**

| Using DHCP | ∨ |

NEXT     Don't have internet connection?
         Skip device setup   ⓘ

a) **Outside Interface**—Ethernet 1/1. You cannot select an alternative outside interface during initial device setup.

**Configure IPv4**—If you need PPPoE, you can configure it after you complete the wizard.

**Configure IPv6**

b) **Management Interface**—Sets parameters for the dedicated Management 1/1 interface. If you changed the IP address at the CLI, you will not see these settings because you already configured them.

**DNS Servers**—The default is the OpenDNS public DNS servers.

**Firewall Hostname**

c) Click **Next**.

**Step 3**     Configure the system time settings.

***Figure 10: Time Setting (NTP)***

Time Setting (NTP)

System Time: 11:56:20AM October 03 2024 -06:00

Time Zone for Scheduling Tasks

(UTC+00:00) UTC

NTP Time Server

Default NTP Servers

Server Name

0.sourcefire.pool.ntp.org

1.sourcefire.pool.ntp.org

2.sourcefire.pool.ntp.org

NEXT

a)  **Time Zone**
b)  **NTP Time Server**
c)  Click **Next**.

**Step 4**   Configure Smart Licensing.

## Register with Cisco Smart Software Manager

Register with Cisco Smart Software Manager to use the full functionality of this device and to apply subscription licenses.

What is smart license? ⌕

○ **Continue with evaluation period:** *Start 90-day evaluation period without registration*
**Recommended if device will be cloud managed.** Learn More ⌕

   Please make sure you register with Cisco before the evaluation period ends. Otherwise you will not be able to make any changes to the device configuration.

◉ **Register device with Cisco Smart Software Manager**

   Please register your device at this time. If you do not register now, you can register later from the Device > Smart License page.

   ① Create or log in into your Cisco Smart Software Manager account.

   ② On your assigned virtual account, under "General tab", click on **"New Token"** to create token.

   ③ Copy the token and paste it here:

   Token

MDM4MTdhNWEtNmExMC00NzMyLWE3YWMtMzY1MWViOTM2Nm
E0LTE3NDU0MzI2%0ANjQyMjV8dUNPZnRLWDJhSFJ6bWc0YkFqVW
ZWQzJzd2JDN2dwRkxhbUhQeHhj%0AZUtnUT0%3D%0A

   ④ Select the region in which your device is operating.

   Region

   US Region ⌄   ⓘ

   ⑤ Enroll Cisco Success Network.

   Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support.This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

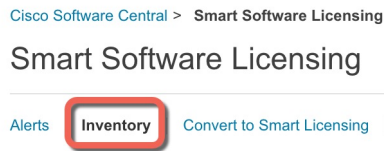   Check out the Sample Data that will be sent to Cisco. See more ⌄

   ☑ Enroll Cisco Success Network

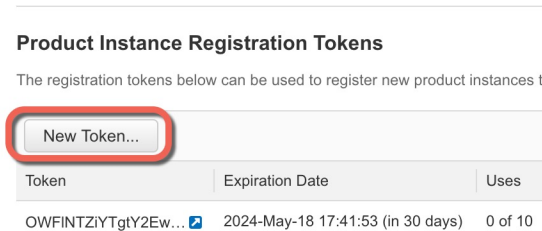   ? For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide ⌕

BACK     FINISH

a) Click **Register device with Cisco Smart Software Manager**.
b) Click the Cisco Smart Software Manager link.
c) Click **Inventory**.

Cisco Software Central > **Smart Software Licensing**

Smart Software Licensing

Alerts | **Inventory** | Convert to Smart Licensing

d) On the **General** tab, click **New Token**.

**Product Instance Registration Tokens**

The registration tokens below can be used to register new product instances t

New Token...

| Token | Expiration Date | Uses |
|---|---|---|
| OWFINTZiYTgtY2Ew... ⤢ | 2024-May-18 17:41:53 (in 30 days) | 0 of 10 |

e) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:

**Create Registration Token**                                    ❓ ✕

This will create a token that is used to register product instances, so that they can use licenses from this virtual account.Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description:                    [Description]

\* Expire After:                 [365]            Days

                              *Between 1 - 365, 30 days recommended*

Max. Number of Uses:            [           ]

                              *The token will be expired when either the expiration or the maximum uses is reached*

☑ Allow export-controlled functionality on the products registered with this token ℹ

                              [Create Token]  [Cancel]

- **Description**

- **Expire After**—Cisco recommends 30 days.

- **Max. Number of Uses**

- **Allow export-controlled functionality on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption. You must select this option now if you plan to use this functionality. If you enable this functionality later, you will need to re-register your device with a new product key and reload the device. If you do not see this option, your account does not support export-controlled functionality.

The token is added to your inventory.

f) Click the arrow icon to the right of the token to open the **Token** dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the threat defense.
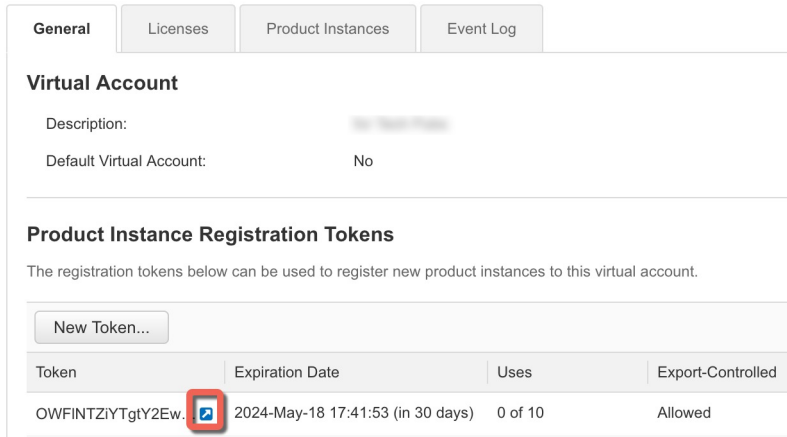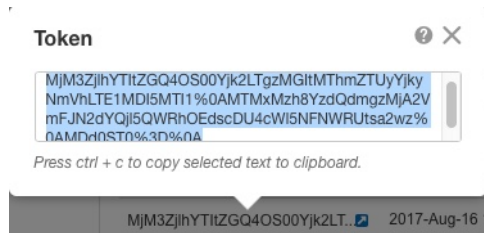
Figure 11: View Token

| General | Licenses | Product Instances | Event Log |
|---------|----------|-------------------|-----------|

**Virtual Account**

Description:

Default Virtual Account: No

**Product Instance Registration Tokens**

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

| Token | Expiration Date | Uses | Export-Controlled |
|-------|-----------------|------|-------------------|
| OWFINTZiYTgtY2Ew. | 2024-May-18 17:41:53 (in 30 days) | 0 of 10 | Allowed |

Figure 12: Copy Token

**Token**

MjM3ZjlhYTltZGQ4OS00Yjk2LTgzMGltMThmZTUyYjky
NmVhLTE1MDl5MTl1%0AMTMxMzh8YzdQdmgzMjA2V
mFJN2dYQjl5QWRhOEdscDU4cWl5NFNWRUtsa2wz%
0AMDd0ST0%3D%0A

Press ctrl + c to copy selected text to clipboard.

MjM3ZjlhYTltZGQ4OS00Yjk2LT..  2017-Aug-16 1

g) In the device manager, paste the token into the token field.

h) Set the other options, and then click **Finish**

**Step 5** Finish the setup wizard.

**Figure 13: What's Next**
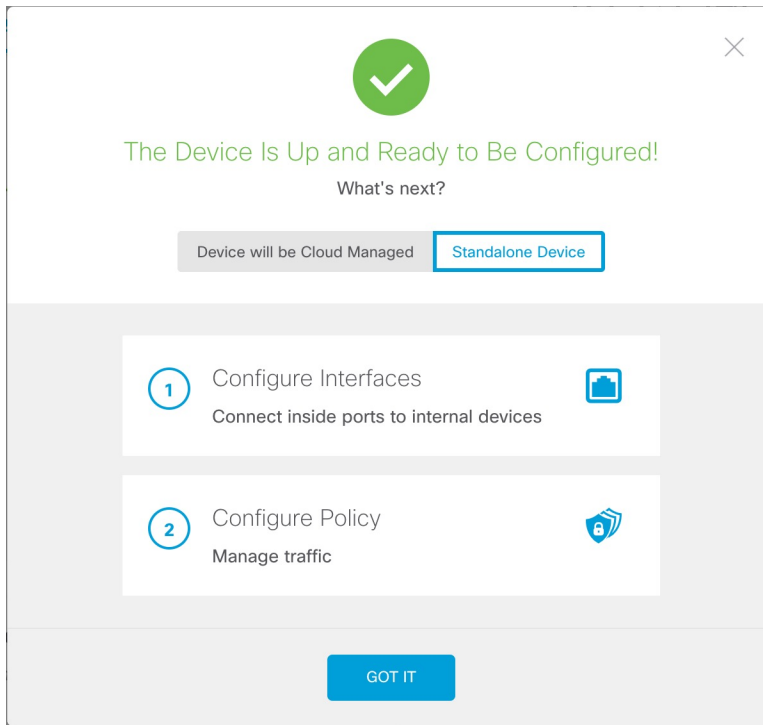


a) Click **Standalone Device** to use the device manager.

b) Click **Configure Interfaces** to go directly to the **Interfaces** page, **Configure Policy** to go to the **Policies** page, or **Got It** to go to the **Device** page.

For interfaces or policy configuration, see Configure the Network Settings and Policy, on page 19.

**Step 6**   Enable feature licenses.

a) From the **Device** page, click **Smart License** > > **View Configuration**.

b) Click the **Enable/Disable** control for each optional license.
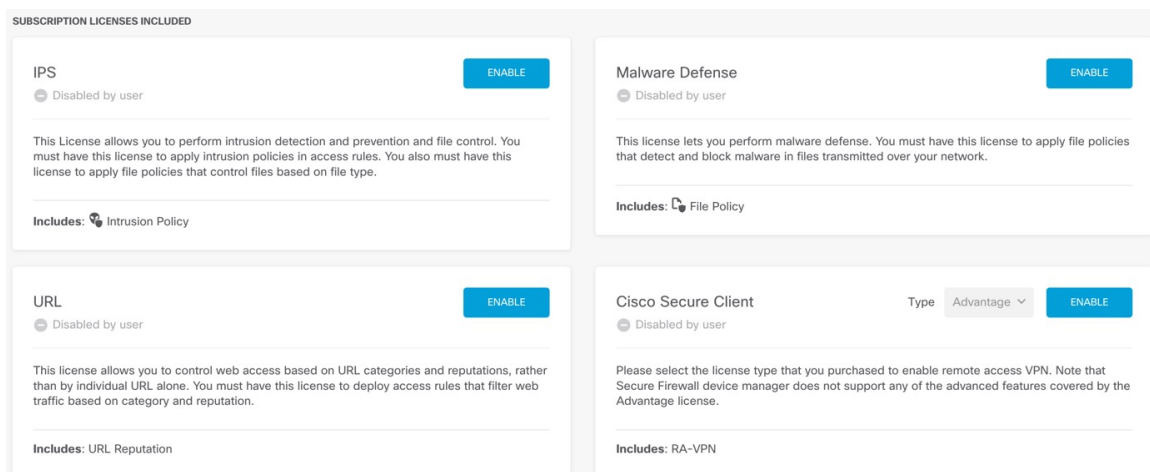
c) Choose **Resync Connection** from the gear drop-down list to synchronize license information with Cisco Smart Software Manager.

Go to Cloud Services ⚙ ⌄

Resync connection

Unregister Device
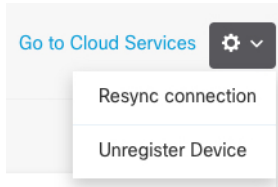
# Configure the Network Settings and Policy

Configure additional interfaces, a DHCP server, and customize the security policy.

**Procedure**

**Step 1**    If you want to convert a switch port to a firewall interface, choose **Device**, and then click the link in the **Interfaces** summary.

a) Click the edit icon (  ) for the switch port.
b) Change the mode from **Switch Port** to **Routed**.

**Figure 14: Change the Mode**



c)   Set the name and IP address.
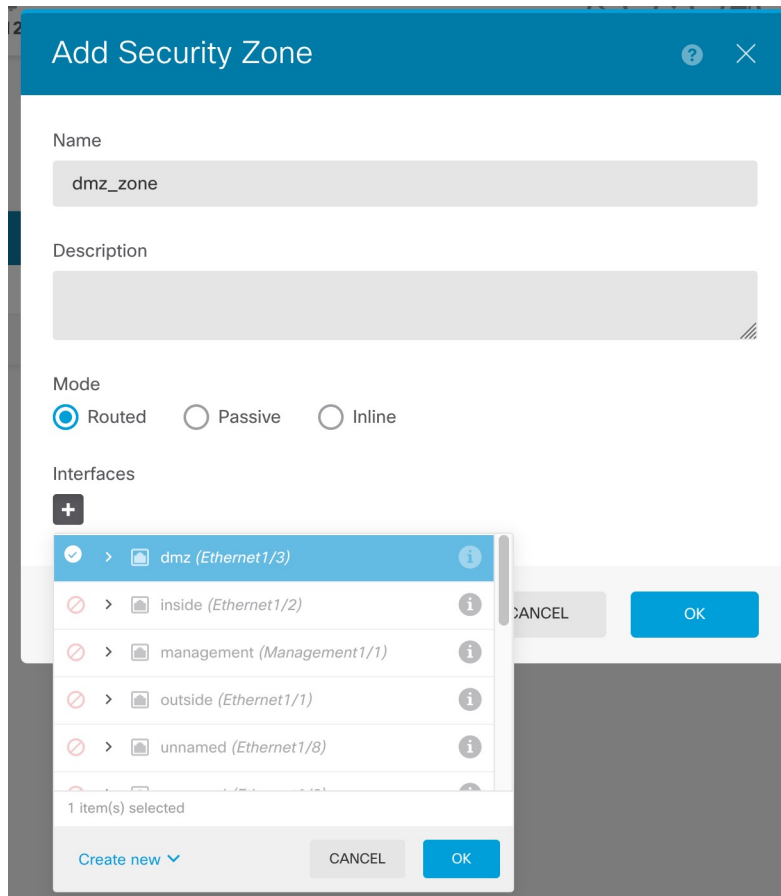
**Figure 15: Edit Interface**



d) Click **OK**.

**Step 2** If you configured new firewall interfaces, choose **Objects**, then select **Security Zones**.

Edit or create new zones as appropriate and assign the interface to the zone. Each interface must belong to a zone for which you configure policies.

The following example creates a new dmz_zone and then assigns the dmz interface to it.

**Figure 16: Security Zone Object**



**Step 3**   If you want internal clients to use DHCP to obtain an IP address from the device, choose **Device** > **System Settings** > **DHCP Server**, then select the **DHCP Servers** tab.

There is already a DHCP server configured for the inside interface.

**Figure 17: DHCP Server**



**Step 4**     Choose **Policies** and configure the security policies for the network.

The device setup wizard enables traffic flow between the inside_zone and outside_zone using a Trust rule. A Trust rule does not apply an intrusion policy. To use intrusion, specify the Allow action for the rule. The policy also includes interface PAT for all interfaces when going to the outside interface.

**Figure 18: Default Security Policies**



However, if you have interfaces in different zones, you need access control rules to allow traffic to and from those zones.

In addition, you can configure other policies to provide additional services and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies by clicking the policy type in the toolbar:

- **SSL Decryption**—If you want to inspect encrypted connections (such as HTTPS) for intrusions, malware, and so forth, you must decrypt the connections. Use the SSL decryption policy to determine which connections need to be decrypted. The system re-encrypts the connection after inspecting it.

- **Identity**—If you want to correlate network activity to individual users, or control network access based on user or user group membership, use the identity policy to determine the user associated with a given source IP address.

- **Security Intelligence**—(Requires the IPS license) Use the Security Intelligence policy to quickly drop connections from or to blacklisted IP addresses or URLs. By blacklisting known bad sites, you do not need to account for them in your access control policy. Cisco provides regularly updated feeds of known bad addresses and URLs so that the Security Intelligence blacklist updates dynamically. Using feeds, you do not need to edit the policy to add or remove items in the blacklist.

- **NAT (Network Address Translation)**—Use the NAT policy to convert internal IP addresses to externally routeable addresses.

- **Access Control**—Use the access control policy to determine which connections are allowed on the network. You can filter by security zone, IP address, protocol, port, application, URL, user or user group. You also apply intrusion and file (malware) policies using access control rules. Use this policy to implement URL filtering.

- **Intrusion**—Use the intrusion policies to inspect for known threats. Although you apply intrusion policies using access control rules, you can edit the intrusion policies to selectively enable or disable specific intrusion rules.

The following example shows how to allow traffic between the inside_zone and dmz_zone in the access control policy. In this example, no options are set on any of the other tabs except for **Logging**, where **At End of Connection** is selected.

*Figure 19: Access Control Policy*
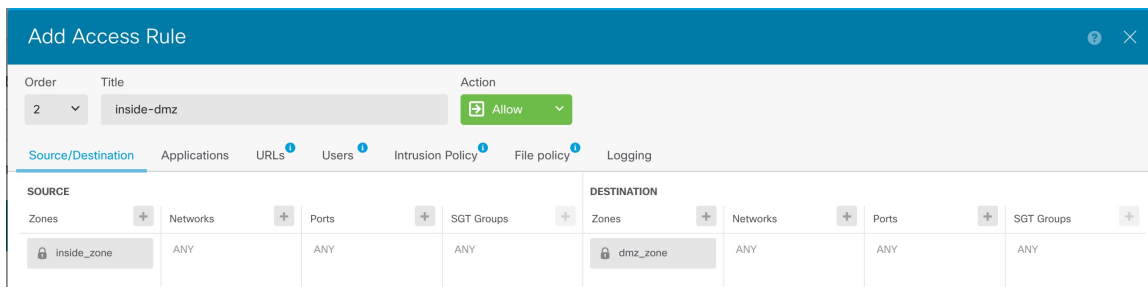


**Step 5**    Choose **Device**, then click **View Configuration** in the **Updates** group and configure the update schedules for the system databases.

If you are using intrusion policies, set up regular updates for the Rules and VDB databases. If you use Security Intelligence feeds, set an update schedule for them. If you use geolocation in any security policies as matching criteria, set an update schedule for that database.

**Step 6**    Click the **Deploy** button in the menu, then click the **Deploy Now** button (  ) to deploy your changes to the device.

Changes are not active on the device until you deploy them.