



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 Firewall Device Manager, on page 1](#)
- [Complete the initial configuration, on page 1](#)
- [Configure the network settings and policy, on page 9](#)

Log Into the Firewall Device Manager

Log into the Firewall Device Manager to configure your Firewall Threat Defense.

Procedure

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

- Ethernet 1/2—<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 Firewall 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:

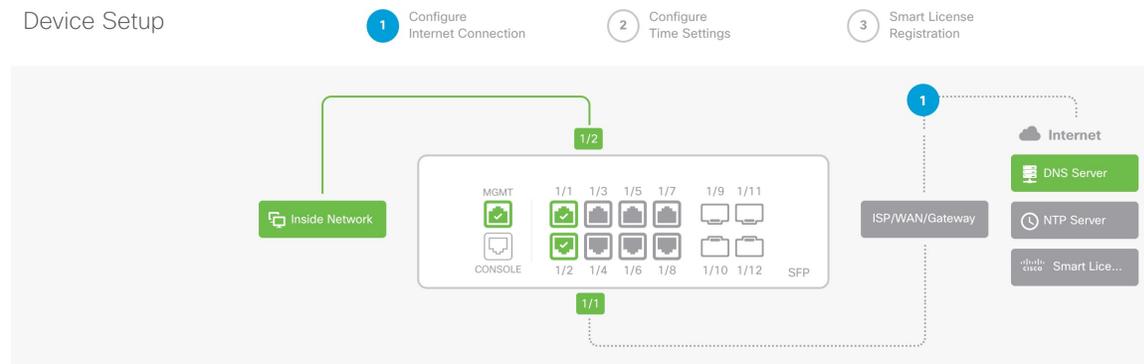
- inside→outside traffic flow
- Interface PAT for all traffic to outside.

Procedure

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

The **Device Setup** screen appears.

Figure 1: Device Setup



Note

The exact port configuration depends on your model.

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

Figure 2: 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.

<p>Rule 1 Trust Outbound Traffic</p> <p>This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.</p>	<p>Default Action Block all other traffic</p> <p>The default action blocks all other traffic.</p>
--	--

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 3: 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 ▼ i

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

```
MDM4MTdhNWEtNmExMC00NzMyLWE3YWMtMzY1MWVlOTM2Nm
E0LTE3NDU0MzI2%0ANjQyMjV8dUNPZnRLWDJhSFJ6bWc0YkFqVW
ZWQzJzd2JDN2dwRkxhbUhhQeHh%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 ↗

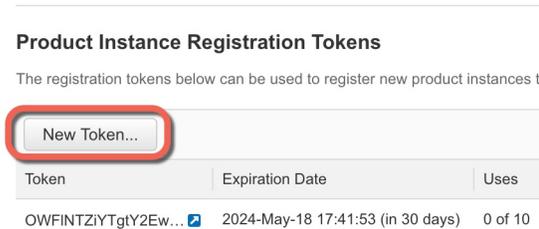
BACK

FINISH

- Click **Register device with Cisco Smart Software Manager**.
- Click the [Cisco Smart Software Manager](#) link.
- Click **Inventory**.



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



- 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:

* Expire After: 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 ?

- **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 Firewall Threat Defense.

Figure 4: View Token

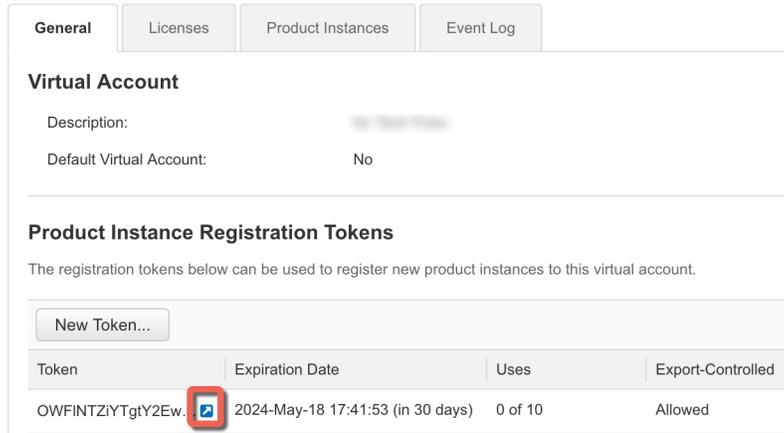
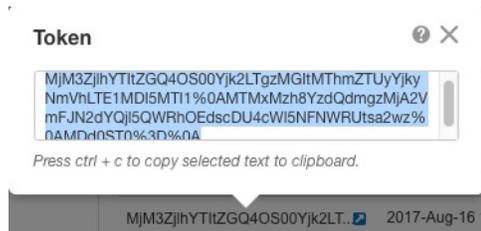


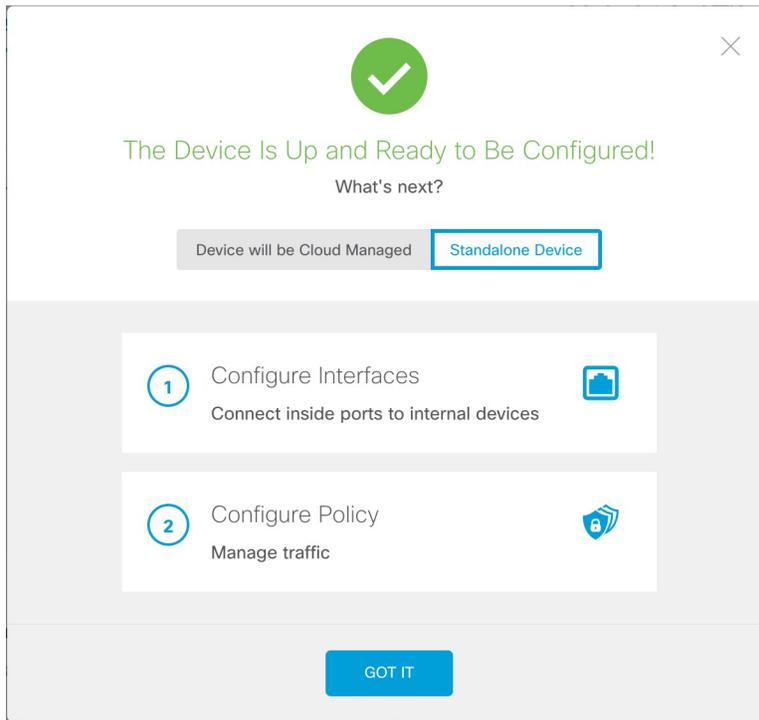
Figure 5: Copy Token



- g) In the Firewall 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 6: What's Next

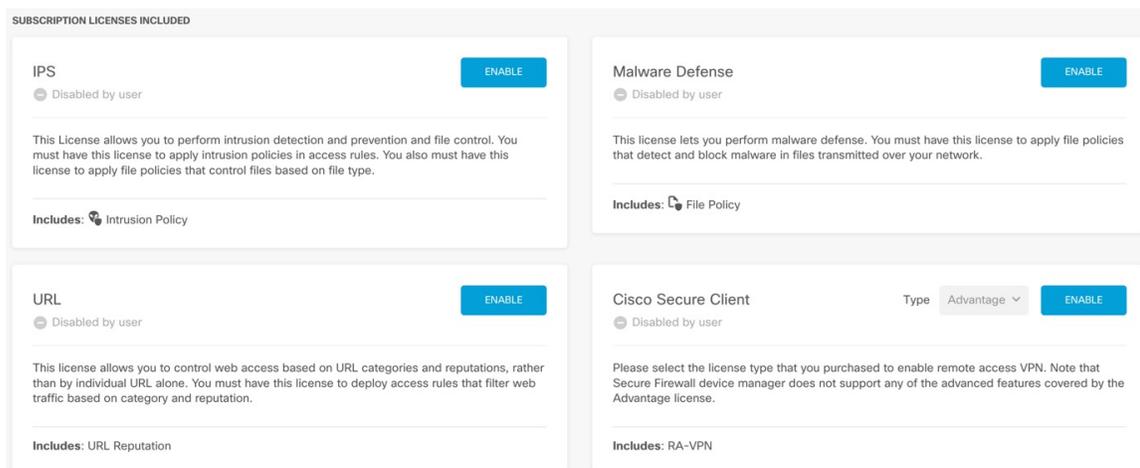


- Click **Standalone Device** to use the Firewall Device Manager.
- Click **Configure Interfaces** to go directly to the **Interfaces** page, **Configure Policy** to go to the **Policies** page, or **Got It** to go to the **Device** page.

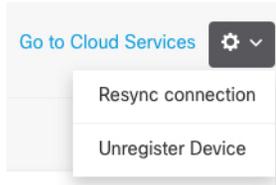
For interfaces or policy configuration, see [Configure the network settings and policy, on page 9](#).

Step 6 Enable feature licenses.

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



Configure the network settings and policy

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

Procedure

Step 1 If you wired other interfaces, choose **Device**, and then click the link in the **Interfaces** summary.

Click the edit icon (🔧) for each interface to define the name, IP address, and other settings.

The following example configures an interface to be used as a “demilitarized zone” (DMZ), where you place publicly-accessible assets such as your web server.

Figure 7: Edit Interface

Ethernet1/3
Edit Physical Interface

Interface Name: Mode: Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

IPv4 Address | IPv6 Address | Advanced

Type:

IP Address and Subnet Mask: /
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask: /
e.g. 192.168.5.16

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 8: Security Zone Object

The screenshot shows the 'Add Security Zone' configuration window. The 'Name' field is filled with 'dmz_zone'. The 'Description' field is empty. Under 'Mode', the 'Routed' radio button is selected. The 'Interfaces' section has a plus sign button. A modal window is open over the plus sign, showing a list of interfaces: 'dmz (Ethernet1/3)' (checked), 'inside (Ethernet1/2)', 'management (Management1/1)', 'outside (Ethernet1/1)', and 'unnamed (Ethernet1/8)'. The modal also shows '1 item(s) selected' and 'Create new' dropdown, 'CANCEL', and 'OK' buttons.

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 9: 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 10: Default Security Policies

#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS	ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS				
1	Inside_Outside...	Trust	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	

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

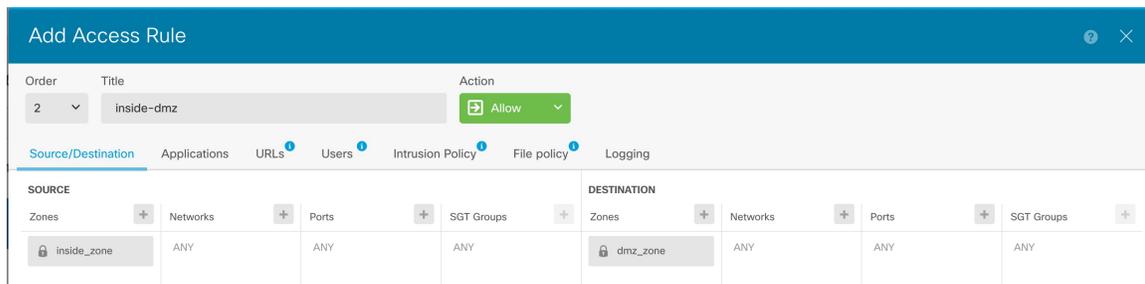
In addition, you can configure other policies to provide additional services and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies by clicking the policy type in the toolbar:

- **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 11: 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.

