



# Configure the Firepower Management Center

Before you can manage devices and control access to the network, you must configure the Firepower Management Center with additional internet settings and a license.

- [Configure the Firepower Management Center for the First Time, on page 1](#)
- [License the Firepower Management Center, on page 4](#)

## Configure the Firepower Management Center for the First Time

### Before you begin

See [Connect the Firepower Management Center to the Network](#).

**Step 1** In your browser's address or location field, enter `https://10.10.2.2`.

**Step 2** Log in with username `admin` and password `Admin123`.  
An initial configuration page is displayed. The following steps walk you through the configuration one section at a time.

**Step 3** Enter a new Firepower Management Center password in the following fields.

**Change Password**

Use these fields to change the password for the admin account. Cisco recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password	<input type="text"/>
Confirm	<input type="text"/>

**Step 4** Enter the network settings shown in the following figure. Enter DNS server specific to your organization, if applicable.

**Network Settings**

Use these fields to specify network-related information for the management interface on the appliance.

Protocol	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Both
IPv4 Management IP	<input type="text" value="10.10.2.2"/>
Netmask	<input type="text" value="255.255.255.0"/>
IPv4 Default Network Gateway	<input type="text" value="10.10.2.254"/>
Hostname	<input type="text" value="firepower"/>
Domain	<input type="text"/>
Primary DNS Server	<input type="text" value="8.8.8.8"/>
Secondary DNS Server	<input type="text"/>
Tertiary DNS Server	<input type="text"/>

**Time Settings**

**Step 5** Enter the time server and time zone settings shown in the following figure. If necessary, click **America/New York** and follow the prompts on your screen to select a time zone.

**Time Settings**

Use these fields to specify how you want to set the time for the Defense Center.

Set My Clock	<input checked="" type="radio"/> Via NTP from <input type="text" value="0.sourcefire.pool.ntp.org, 1.sourcefire.org"/>
	<input type="radio"/> Manually <input type="text" value="2018"/> / <input type="text" value="March"/> / <input type="text" value="28"/> : <input type="text" value="13"/> : <input type="text" value="15"/>
Current Time	2018-03-28 14:06
Set Display Time Zone	<input type="text" value="America/New York"/>

**Step 6** Select options for recurring updates and automatic backup:

- **Recurring Rule Update Imports:** As new vulnerabilities become known, the Vulnerability Research Team (VRT) releases intrusion rule updates. Rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates might also delete rules and provide new rule categories and system variables.

You can specify the **Import Frequency**, as well as configure the system to perform an intrusion **Policy Reapply** after each rule update. To perform a rule update as part of the initial configuration process, check **Install Now**.

Rule updates might contain new binaries. Make sure your process for downloading and installing rule updates complies with your security policies. In addition, rule updates may be large, so make sure to import rules during periods of low network use.

- **Recurring Geolocation Updates:** Firepower Management Centers can display geographical information about the routed IP addresses associated with events generated by the system, as well as monitor geolocation statistics in the dashboard and Context Explorer.

The Firepower Management Center's geolocation database (GeoDB) contains information such as an IP address's associated Internet service provider (ISP), connection type, proxy information, and exact location. Enabling regular GeoDB updates ensures that the system uses up-to-date geolocation information.

You can specify the weekly update frequency for the GeoDB. To download the database as part of the initial configuration process, check **Install Now**.

GeoDB updates might take up to 45 minutes to install after download. You should update the GeoDB during periods of low network use.

- **Enable Automatic Backups:** Creates a scheduled task that creates a weekly backup of the configurations on the Firepower Management Center.

**Recurring Rule Update Imports**

Use these fields to schedule recurring rule updates.

Install Now

Enable Recurring Rule Update Imports from the Support Site

**Recurring Geolocation Updates**

Use these fields to schedule recurring weekly geolocation updates. Note that updates may be large and can take up to 45 minutes.

Install Now

Enable Recurring Weekly Updates from the Support Site

**Automatic Backups**

Use this field to schedule automatic configuration backups.

Enable Automatic Backups

**Step 7** Leave the License Settings section blank because it applies to Classic licenses only; you'll apply a Smart License later.

**License Settings**

To obtain your license, navigate to <https://www.cisco.com/go/license/> where you will be prompted for the license key (66:00:50:56:8D:1A:5D) and the activation key, which was emailed to the contact person on your support contract. Follow the on-screen instructions to generate a license, which will be emailed to you. Paste the license below and click Add/Verify. If your browser cannot access the Internet, switch to a host that can.

License Key 66:00:50:56:8D:1A:5D

**Step 8** Scroll through the license agreement and, if you agree, check **I have read and agree to the End User License Agreement** and click **Apply**.

**End User License Agreement**

End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof.

This agreement, any supplemental license terms and any specific product terms at [www.cisco.com/go/softwareterms](http://www.cisco.com/go/softwareterms) (collectively, the "EULA") govern Your Use of the Software.

1. **Acceptance of Terms. By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on**

I have read and agree to the End User License Agreement.

**Step 9** Wait until the Firepower Management Center processes the information you entered. At that point, the Dashboard is displayed.

**What to do next**

See [License the Firepower Management Center, on page 4](#).

# License the Firepower Management Center

This task discusses how to use a 90-day evaluation license with the Firepower Management Center and managed devices. If you have a Smart License, you can use it instead.

- Step 1** If necessary, log in to the Firepower Management Center.
- Step 2** Click **System > Licenses > Smart Licenses**.
- Step 3** Click **Evaluation Mode** for a 90-day evaluation license or click **Register** to register with a Smart License.

**Welcome to Smart Licenses**

Before you use Smart Licenses, obtain a registration token from [Cisco Smart Software Manager](#), then click Register

Register
Evaluation Mode

- Step 4** If you are using an evaluation license, click **Yes** to start the 90-day evaluation period. If you selected an evaluation license, the following page is displayed.

**Smart License Status** [Cisco Smart Software Manager](#)

---

Usage Authorization:	N/A	
Product Registration:	<span style="color: green;">✔</span>	Evaluation Period (Expires in 89 days)
Assigned Virtual Account:		Evaluation Mode
Export-Controlled Features:		Disabled
Cisco Success Network:		Disabled <span style="color: blue;">i</span>

  

**Smart Licenses** Filter Devices...  Edit Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
<b>Base (0)</b>				
<b>Malware (0)</b>				
<b>Threat (0)</b>				
<b>URL Filtering (0)</b>				
<b>AnyConnect Apex (0)</b>				
<b>AnyConnect Plus (0)</b>				
<b>AnyConnect VPN Only (0)</b>				

**What to do next**

See [Configure the Managed Device](#).