Cisco Firepower is an integrated suite of network security and traffic management products, deployed either on purpose-built platforms or as a software solution. The system is designed to help you handle network traffic in a way that complies with your organization’s security policy—your guidelines for protecting your network.

In a typical deployment, multiple traffic-sensing managed devices installed on network segments monitor traffic for analysis and report to a manager:

- Firepower Management Center
- Firepower Device Manager
- Adaptive Security Device Manager (ASDM)

Managers provide a centralized management console with graphical user interface that you can use to perform administrative, management, analysis, and reporting tasks.

This guide focuses on the Firepower Management Center managing appliance. For information about the Firepower Device Manager or ASA with FirePOWER Services managed via ASDM, see the guides for those management methods.

- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager
- ASA with FirePOWER Services Local Management Configuration Guide

- Quick Start: Basic Setup, on page 2
- Firepower Devices, on page 6
- Firepower Features, on page 6
- Switching Domains on the Firepower Management Center, on page 11
- The Context Menu, on page 12
- Sharing Data with Cisco, on page 13
- Firepower Online Help, How To, and Documentation, on page 14
- Firepower System IP Address Conventions, on page 17
- Additional Resources, on page 17
Quick Start: Basic Setup

The Firepower feature set is powerful and flexible enough to support basic and advanced configurations. Use the following sections to quickly set up a Firepower Management Center and its managed devices to begin controlling and analyzing traffic.

Installing and Performing Initial Setup on Physical Appliances

Install and perform initial setup on all physical appliances using the documentation for your appliance:

- **Firepower Management Center**

- **Firepower Threat Defense managed devices**

  **Important** Ignore Firepower Device Manager documents on these pages.

  - Firepower Threat Defense for the 1010: *Cisco Firepower Threat Defense for the Firepower 1010 Using Firepower Management Center Quick Start Guide*
    http://www.cisco.com/go/ftd-quick

  - Firepower Threat Defense for the 1120 and 1140: *Cisco Firepower Threat Defense for the Firepower 1120 and 1140 Using Firepower Management Center Quick Start Guide*
    http://www.cisco.com/go/ftd-quick

  - Firepower Threat Defense for the 2100: *Cisco Firepower Threat Defense for the Firepower 2100 Series Using Firepower Management Center Quick Start Guide*
    http://www.cisco.com/go/ftd-quick

  - Firepower Threat Defense for the 4100: *Cisco Firepower Threat Defense for Firepower 4100 Quick Start Guide*
    http://www.cisco.com/go/ftd-quick

  - Firepower Threat Defense for the 9300: *Cisco Firepower Threat Defense for Firepower 9300 Quick Start Guide*
    http://www.cisco.com/go/ftd-quick

  - Firepower Threat Defense for the ASA 5508-X/5516-X: *Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide*
    http://www.cisco.com/go/ftd-quick

    http://www.cisco.com/go/ftd-quick

  - Firepower Threat Defense for the ISA 3000: *Cisco Firepower Threat Defense for the ISA 3000 Using Firepower Management Center Quick Start Guide*
http://www.cisco.com/go/ftd-quick

- **Classic managed devices**
  - ASA FirePOWER Services managed device: *Cisco ASA FirePOWER Module Quick Start Guide*
    http://www.cisco.com/go/asafp-quick
  - 8000 Series managed device: *Cisco Firepower 8000 Series Getting Started Guide*
    http://www.cisco.com/go/8000series-install
  - 7000 Series managed device: *Cisco Firepower 7000 Series Getting Started Guide*
    http://www.cisco.com/go/7000series-install

---

### Deploying Virtual Appliances


---

**Step 1** Determine the supported virtual platforms you will use for the Management Center and devices (these may not be the same). See the *Cisco Firepower Compatibility Guide*.

**Step 2** Deploy virtual Firepower Management Centers using the documentation for your environment:

- Firepower Management Center Virtual running on VMware: *Cisco Firepower Management Center Virtual for VMware Deployment Quick Start Guide*
- Firepower Management Center Virtual running on AWS: *Cisco Firepower Management Center Virtual for AWS Deployment Quick Start Guide*
- Firepower Management Center Virtual running on KVM: *Cisco Firepower Management Center Virtual for KVM Deployment Quick Start Guide*

**Step 3** Deploy virtual devices using the documentation for your appliance:

- NGIPSv running on VMware: *Cisco Firepower NGIPSv Quick Start Guide for VMware*
- Firepower Threat Defense Virtual running on VMware: *Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide*
- Firepower Threat Defense Virtual running on AWS: *Cisco Firepower Threat Defense Virtual for AWS Deployment Quick Start Guide*
- Firepower Threat Defense Virtual running on KVM: *Cisco Firepower Threat Defense Virtual for KVM Deployment Quick Start Guide*
- Firepower Threat Defense Virtual running on Azure: *Cisco Firepower Threat Defense Virtual for Azure Deployment Quick Start Guide*
Logging In for the First Time

Before you begin

• Prepare your appliances as described in Installing and Performing Initial Setup on Physical Appliances, on page 2 or Deploying Virtual Appliances, on page 3.

Step 1
Log in to the Firepower Management Center web interface with admin as the username and Admin123 as the password. Change the password for this account as described in the Quick Start Guide for your appliance.

Step 2
Set a time zone for this account as described in Setting Your Default Time Zone.

Step 3
Add licenses as described in Licensing the Firepower System.

Step 4
Register managed devices as described in Add Devices to the Firepower Management Center.

Step 5
Configure your managed devices as described in:

• Introduction to IPS Device Deployment and Configuration, to configure passive or inline interfaces on 7000 Series or 8000 Series devices
• Interface Overview for Firepower Threat Defense, to configure transparent or routed mode on Firepower Threat Defense devices
• Interface Overview for Firepower Threat Defense, to configure interfaces on Firepower Threat Defense devices

What to do next

• Begin controlling and analyzing traffic by configuring basic policies as described in Setting Up Basic Policies and Configurations, on page 4.

Setting Up Basic Policies and Configurations

You must configure and deploy basic policies in order to see data in the dashboard, Context Explorer, and event tables.

Note
This is not a full discussion of policy or feature capabilities. For guidance on other features and more advanced configurations, see the rest of this guide.

Before you begin

• Log into the web interface, set your time zone, add licenses, register devices, and configure devices as described in Logging In for the First Time, on page 4.

Step 1
Configure an access control policy as described in Creating a Basic Access Control Policy.
• In most cases, Cisco suggests setting the Balanced Security and Connectivity intrusion policy as your default action. For more information, see Access Control Policy Default Action and System-Provided Network Analysis and Intrusion Policies.

• In most cases, Cisco suggests enabling connection logging to meet the security and compliance needs of your organization. Consider the traffic on your network when deciding which connections to log so that you do not clutter your displays or overwhelm your system. For more information, see About Connection Logging.

Step 2 Apply the system-provided default health policy as described in Applying Health Policies.

Step 3 Customize a few of your system configuration settings:

• If you want to allow inbound connections for a service (for example, SNMP or the syslog), modify the ports in the access list as described in Configuring the Access List for Your System.

• Understand and consider editing your database event limits as described in Configuring Database Event Limits.

• If you want to change the display language, edit the language setting as described in Specifying a Different Language.

• If your organization restricts network access using a proxy server and you did not configure proxy settings during initial configuration, edit your proxy settings as described in Configure Firepower Management Center Management Interfaces.

Step 4 Customize your network discovery policy as described in Configuring the Network Discovery Policy. By default, the network discovery policy analyzes all traffic on your network. In most cases, Cisco suggests restricting discovery to the addresses in RFC 1918.

Step 5 Consider customizing these other common settings:

• If you do not want to display message center pop-ups, disable notifications as described in Configuring Notification Behavior.

• If you want to customize the default values for system variables, understand their use as described in Variable Sets.

• If you want to update the Geolocation Database, update manually or on a scheduled basis as described in Update the Geolocation Database (GeoDB).

• If you want to create additional locally authenticated user accounts to access the appliance, see Add an Internal User Account.

• If you want to use LDAP or RADIUS external authentication to allow access to the appliance, see Configure External Authentication.

Step 6 Deploy configuration changes; see Deploy Configuration Changes.

What to do next

• Review and consider configuring other features described in Firepower Features, on page 6 and the rest of this guide.
Firepower Devices

In a typical deployment, multiple traffic-handling devices report to one Firepower Management Center, which you use to perform administrative, management, analysis, and reporting tasks.

Classic Devices

Classic devices run next-generation IPS (NGIPS) software. They include:

- Firepower 7000 series and Firepower 8000 series physical devices.
- NGIPSv, hosted on VMware.
- ASA with FirePOWER Services, available on select ASA 5500-X series devices (also includes ISA 3000). The ASA provides the first-line system policy, and then passes traffic to an ASA FirePOWER module for discovery and access control.

Note that you must use the ASA CLI or ASDM to configure the ASA-based features on an ASA FirePOWER device. This includes device high availability, stacking, switching, routing, VPN, NAT, and so on. You cannot use the FMC to configure ASA FirePOWER interfaces, and the FMC GUI does not display ASA interfaces when the ASA FirePOWER is deployed in SPAN port mode. Also, you cannot use the FMC to shut down, restart, or otherwise manage ASA FirePOWER processes.

Firepower Threat Defense Devices

A Firepower Threat Defense (FTD) device is a next-generation firewall (NGFW) that also has NGIPS capabilities. NGFW and platform features include site-to-site and remote access VPN, robust routing, NAT, clustering, and other optimizations in application inspection and access control.

FTD is available on a wide range of physical and virtual platforms.

Compatibility

For details on manager-device compatibility, including the software compatible with specific device models, virtual hosting environments, operating systems, and so on, see the Cisco Firepower Release Notes and Cisco Firepower Compatibility Guide.

Firepower Features

These tables list some commonly used Firepower features.

Appliance and System Management Features


<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Configure...</th>
<th>As described in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage user accounts for logging in to your Firepower appliances</td>
<td>Firepower authentication</td>
<td>About User Accounts</td>
</tr>
<tr>
<td>If you want to...</td>
<td>Configure...</td>
<td>As described in...</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>---------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>Monitor the health of system hardware and software</td>
<td>Health monitoring policy</td>
<td>About Health Monitoring</td>
</tr>
<tr>
<td>Back up data on your appliance</td>
<td>Backup and restore</td>
<td>Backup and Restore</td>
</tr>
<tr>
<td>Upgrade to a new Firepower version</td>
<td>System updates</td>
<td>Cisco Firepower Management Center Upgrade Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firepower Release Notes</td>
</tr>
<tr>
<td>Baseline your physical appliance</td>
<td>Restore to factory defaults (reimage)</td>
<td>The Cisco Firepower Management Center Upgrade Guide, for a list of links to instructions on performing fresh installations.</td>
</tr>
<tr>
<td>Update the VDB, intrusion rule updates, or GeoDB on your appliance</td>
<td>Vulnerability Database (VDB) updates, intrusion rule updates, or Geolocation Database (GeoDB) updates</td>
<td>System Software Updates</td>
</tr>
<tr>
<td>Apply licenses in order to take advantage of license-controlled functionality</td>
<td>Classic or Smart licensing</td>
<td>About Firepower Licenses</td>
</tr>
<tr>
<td>Ensure continuity of appliance operations</td>
<td>Managed device high availability and/or Firepower Management Center high availability</td>
<td>About 7000 and 8000 Series Device High Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>About Firepower Threat Defense High Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>About Firepower Management Center High Availability</td>
</tr>
<tr>
<td>Combine processing resources of multiple 8000 Series devices</td>
<td>Device stacking</td>
<td>About Device Stacks</td>
</tr>
<tr>
<td>Configure a device to route traffic between two or more interfaces</td>
<td>Routing</td>
<td>Virtual Routers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Routing Overview for Firepower Threat Defense</td>
</tr>
<tr>
<td>Configure packet switching between two or more networks</td>
<td>Device switching</td>
<td>Virtual Switches</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configure Bridge Group Interfaces</td>
</tr>
<tr>
<td>Translate private addresses into public addresses for internet connections</td>
<td>Network Address Translation (NAT)</td>
<td>NAT Policy Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Address Translation (NAT) for Firepower Threat Defense</td>
</tr>
<tr>
<td>Establish a secure tunnel between managed Firepower Threat Defense or 7000/8000 Series devices</td>
<td>Site-to-Site virtual private network (VPN)</td>
<td>VPN Overview for Firepower Threat Defense</td>
</tr>
</tbody>
</table>
If you want to... | Configure... | As described in...
---|---|---
Establish secure tunnels between remote users and managed Firepower Threat Defense devices | Remote Access VPN | VPN Overview for Firepower Threat Defense
Segment user access to managed devices, configurations, and events | Multitenancy using domains | Introduction to Multitenancy Using Domains
View and manage appliance configuration using a REST API client | REST API and REST API Explorer | REST API Preferences
| | Firepower REST API Quick Start Guide
Troubleshoot issues | N/A | Troubleshooting the System

**High Availability and Scalability Features by Platform**

High availability configurations (sometimes called failover) ensure continuity of operations. Clustered and stacked configurations group multiple devices together as a single logical device, achieving increased throughput and redundancy.

<table>
<thead>
<tr>
<th>Platform</th>
<th>High Availability</th>
<th>Clustering</th>
<th>Stacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower Management Center</td>
<td>Yes Except MC750</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firepower Management Center Virtual</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| Firepower Threat Defense:  
• Firepower 1000 series  
• Firepower 2100 series  
• ASA 5500-X series  
• ISA 3000 | Yes | | |
| Firepower Threat Defense:  
• Firepower 4100/9300 chassis | Yes | Yes | |
| Firepower Threat Defense Virtual:  
• VMware  
• KVM | Yes | | |
| Firepower Threat Defense Virtual (public cloud):  
• AWS  
• Azure | | | |
### Platform and High Availability

<table>
<thead>
<tr>
<th>Platform</th>
<th>High Availability</th>
<th>Clustering</th>
<th>Stacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower NGIPS:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Firepower 7010, 7020, 7030, 7050</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>- Firepower 7110, 7115, 7120, 7125</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>- Firepower 8120, 8130</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>- AMP 7150, 8050, 8150</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Firepower NGIPS:</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td>- Firepower 8140</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>- Firepower 8250, 8260, 8270, 8290</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>- Firepower 8350, 8360, 8370, 8390</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>- AMP 8350</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Firepower NGIPS:</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>- ASA FirePOWER</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>- NGIPSv</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

### Related Topics

- About 7000 and 8000 Series Device High Availability
- About Firepower Threat Defense High Availability
- About Firepower Management Center High Availability

### Features for Detecting, Preventing, and Processing Potential Threats


<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Configure...</th>
<th>As described in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspect, log, and take action on network traffic</td>
<td>Access control policy, the parent of several other policies</td>
<td>Introduction to Access Control</td>
</tr>
<tr>
<td>Blacklist connections to or from IP addresses, URLs, and/or domain names</td>
<td>Security Intelligence within your access control policy</td>
<td>About Security Intelligence</td>
</tr>
<tr>
<td>Control the websites that users on your network can access</td>
<td>URL filtering within your policy rules</td>
<td>URL Filtering</td>
</tr>
<tr>
<td>Monitor malicious traffic and intrusions on your network</td>
<td>Intrusion policy</td>
<td>Intrusion Policy Basics</td>
</tr>
</tbody>
</table>
As described in... Configure... As described in...

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Configure...</th>
<th>As described in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block encrypted traffic without inspection</td>
<td>SSL policy</td>
<td>SSL Policies Overview</td>
</tr>
<tr>
<td>Inspect encrypted or decrypted traffic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tailor deep inspection to encapsulated traffic and improve performance with fastpathing</td>
<td>Prefilter policy</td>
<td>About Prefiltering</td>
</tr>
<tr>
<td>Rate limit network traffic that is allowed or trusted by access control</td>
<td>Quality of Service (QoS) policy</td>
<td>About QoS Policies</td>
</tr>
<tr>
<td>Allow or block files (including malware) on your network</td>
<td>File/malware policy</td>
<td>File Policies and Advanced Malware Protection</td>
</tr>
<tr>
<td>Operationalize data from threat intelligence sources</td>
<td>Cisco Threat Intelligence Director (TID)</td>
<td>Cisco Threat Intelligence Director (TID) Overview</td>
</tr>
<tr>
<td>Configure passive or active user authentication to perform user awareness and user control</td>
<td>User awareness, user identity, identity policies</td>
<td>About User Identity Sources About Identity Policies</td>
</tr>
<tr>
<td>Collect host, application, and user data from traffic on your network to perform user awareness</td>
<td>Network Discovery policies</td>
<td>Overview: Network Discovery Policies</td>
</tr>
<tr>
<td>Use external tools to collect and analyze data about network traffic and potential threats</td>
<td>Integration with external tools</td>
<td>Event Analysis Using External Tools</td>
</tr>
<tr>
<td>Perform application detection and control</td>
<td>Application detectors</td>
<td>Overview: Application Detection</td>
</tr>
<tr>
<td>Troubleshoot issues</td>
<td>N/A</td>
<td>Troubleshooting the System</td>
</tr>
</tbody>
</table>

### Integration with External Tools


<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Configure...</th>
<th>As described in...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically launch remediations when conditions on your network violate an associated policy</td>
<td>Remediations</td>
<td>Introduction to Remediations Firepower System Remediation API Guide</td>
</tr>
<tr>
<td>Stream event data from a Firepower Management Center to a custom-developed client application</td>
<td>eStreamer integration</td>
<td>eStreamer Server Streaming Firepower System eStreamer Integration Guide</td>
</tr>
</tbody>
</table>
Switching Domains on the Firepower Management Center

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Device</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>Any</td>
<td>FMC</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

In a multidomain deployment, user role privileges determine which domains a user can access and which privileges the user has within each of those domains. You can associate a single user account with multiple domains and assign different privileges for that user in each domain. For example, you can assign a user read-only privileges in the Global domain, but Administrator privileges in a descendant domain.

Users associated with multiple domains can switch between domains within the same web interface session. Under your user name in the toolbar, the system displays a tree of available domains. The tree:

- Displays ancestor domains, but may disable access to them based on the privileges assigned to your user account.
- Hides any other domain your user account cannot access, including sibling and descendant domains.

When you switch to a domain, the system displays:

- Data that is relevant to that domain only.
- Menu options determined by the user role assigned to you for that domain.

From the drop-down list under your user name, choose the domain you want to access.
The Context Menu

Certain pages in the Firepower System web interface support a right-click (most common) or left-click context menu that you can use as a shortcut for accessing other features in the Firepower System. The contents of the context menu depend where you access it—not only the page but also the specific data.

For example:

• IP address hotspots provide information about the host associated with that address, including any available whois and host profile information.

• SHA-256 hash value hotspots allow you to add a file’s SHA-256 hash value to the clean list or custom detection list, or view the entire hash value for copying.

On pages or locations that do not support the Firepower System context menu, the normal context menu for your browser appears.

Policy Editors

Many policy editors contain hotspots over each rule. You can insert new rules and categories; cut, copy, and paste rules; set the rule state; and edit the rule.

Intrusion Rules Editor

The intrusion rules editor contains hotspots over each intrusion rule. You can edit the rule, set the rule state, configure thresholding and suppression options, and view rule documentation. Optionally, after clicking Rule documentation in the context menu, you can click Rule Documentation in the documentation pop-up window to view more-specific rule details.

Event Viewer

Event pages (the drill-down pages and table views available under the Analysis menu) contain hotspots over each event, IP address, URL, DNS query, and certain files’ SHA-256 hash values. While viewing most event types, you can:

• View related information in the Context Explorer.

• Drill down into event information in a new window.

• View the full text in places where an event field contains text too long to fully display in the event view, such as a file’s SHA-256 hash value, a vulnerability description, or a URL.

• Open a web browser window with detailed information about the element from a source external to Firepower, using the Contextual Cross-Launch feature. For more information, see Event Investigation Using Web-Based Resources.

• (If your organization has deployed Cisco Security Packet Analyzer) Explore packets related to the event. For details, see Event Investigation Using Cisco Security Packet Analyzer.

While viewing connection events, you can add items to the default Security Intelligence whitelists and blacklists:

• An IP address, from an IP address hotspot.

• A URL or domain name, from a URL hotspot.

• A DNS query, from a DNS query hotspot.
While viewing captured files, file events, and malware events, you can:

- Add a file to or remove a file from the clean list or custom detection list.
- Download a copy of the file.
- View nested files inside an archive file.
- Download the parent archive file for a nested file.
- View the file composition.
- Submit the file for local malware and dynamic analysis.

While viewing intrusion events, you can perform similar tasks to those in the intrusion rules editor or an intrusion policy:

- Edit the triggering rule.
- Set the rule state, including disabling the rule.
- Configure thresholding and suppression options.
- View rule documentation. Optionally, after clicking Rule documentation in the context menu, you can click Rule Documentation in the documentation pop-up window to view more-specific rule details.

**Intrusion Event Packet View**

Intrusion event packet views contain IP address hotspots. The packet view uses a left-click context menu.

**Dashboard**

Many dashboard widgets contain hotspots to view related information in the Context Explorer. Dashboard widgets can also contain IP address and SHA-256 hash value hotspots.

**Context Explorer**

The Context Explorer contains hotspots over its charts, tables, and graphs. If you want to examine data from graphs or lists in more detail than the Context Explorer allows, you can drill down to the table views of the relevant data. You can also view related host, user, application, file, and intrusion rule information.

The Context Explorer uses a left-click context menu, which also contains filtering and other options unique to the Context Explorer.

**Related Topics**

- Security Intelligence Lists and Feeds

**Sharing Data with Cisco**

You can opt to share data with Cisco using the following features:

- Cisco Success Network
  - See Cisco Success Network
- Web analytics
  - See (Optional) Opt Out of Web Analytics Tracking
Firepower Online Help, How To, and Documentation

You can reach the online help from the web interface:

• By clicking the context-sensitive help link on each page

• By choosing Help > Online

How To is a widget that provides walkthroughs to navigate through tasks on Firepower Management Center. The walkthroughs guide you to perform the steps required to achieve a task by taking you through each step, one after the other irrespective of the various UI screens that you may have to navigate, to complete the task. The How To widget is enabled by default. To disable the widget, choose User Preferences from the drop-down list under your user name, and deselect the Enable How-Tos checkbox in the How-To Settings tab.

Note

The walkthroughs are generally available for all UI pages, and are not user role sensitive. However, depending on the privileges of the user, some of the menu items will not appear on the Firepower Management Center interface. Thereby, the walkthroughs will not execute on such pages.

The following walkthroughs are available on Firepower Management Center:

• Register FMC with Cisco Smart Account: This walkthrough guides you to register Firepower Management Center with Cisco Smart Account.

• Set up a Device and add it to FMC: This walkthrough guides you to set up a device and to add the device to Firepower Management Center.

• Configure Date and Time: This walkthrough guides you to configure the date and time of the Firepower Threat Defense devices using a platform settings policy.

• Configure Interface Settings: This walkthrough guides you to configure the interfaces on the Firepower Threat Defense devices.

• Create an Access Control Policy: An access control policy consists of a set of ordered rules, which are evaluated from top to bottom. This walkthrough guides you to create an access control policy.

• Add an Access Control Rule - A Feature Walkthrough: This walkthrough describes the components of an access control rule, and how you can use them in Firepower Management Center.

• Configure Routing Settings: Various routing protocols are supported by Firepower Threat Defense. A static route defines where to send traffic for specific destination networks. This walkthrough guides you to configure static routing for the devices.

• Create a NAT Policy - A Feature Walkthrough: This walkthrough guides you to create a NAT policy and walks you through the various features of a NAT rule.

Top-Level Documentation Listing Pages for FMC Deployments

The following documents may be helpful when configuring Firepower Management Center deployments, Version 6.0+

Some of the linked documents are not applicable to Firepower Management Center deployments. For example, some links on Firepower Threat Defense pages are specific to deployments managed by Firepower Device Manager, and some links on hardware pages are unrelated to Firepower. To avoid confusion, pay careful attention to document titles. Also, some documents cover multiple products and therefore may appear on multiple product pages.

Firepower Management Center

• Firepower Management Center hardware appliances:

• Firepower Management Center Virtual appliances:
    tsd-products-support-series-home.html

Firepower Threat Defense, also called NGFW (Next Generation Firewall) devices

• Firepower Threat Defense software:

• Firepower Threat Defense Virtual:
    tsd-products-support-series-home.html

• Firepower 1000 series:
    tsd-products-support-series-home.html

• Firepower 2100 series:
    tsd-products-support-series-home.html

• Firepower 4100 series:
    tsd-products-support-series-home.html

• Firepower 9300:
    tsd-products-support-series-home.html
License Statements in the Documentation

The License statement at the beginning of a section indicates which Classic or Smart license you must assign to a managed device in the Firepower System to enable the feature described in the section.

Because licensed capabilities are often additive, the license statement provides only the highest required license for each feature.
An “or” statement in a License statement indicates that you must assign a particular license to the managed device to enable the feature described in the section, but an additional license can add functionality. For example, within a file policy, some file rule actions require that you assign a Protection license to the device while others require that you assign a Malware license.

For more information about licenses, see About Firepower Licenses.

**Related Topics**

- About Firepower Licenses

---

**Supported Devices Statements in the Documentation**

The Supported Devices statement at the beginning of a chapter or topic indicates that a feature is supported only on the specified device series, family, or model. For example, stacking is supported only on 8000 Series devices.

For more information on platforms supported by this release, see the release notes.

---

**Access Statements in the Documentation**

The Access statement at the beginning of each procedure in this documentation indicates the predefined user roles required to perform the procedure. Any of the listed roles can perform the procedure.

Users with custom roles may have permission sets that differ from those of the predefined roles. When a predefined role is used to indicate access requirements for a procedure, a custom role with similar permissions also has access. Some users with custom roles may use slightly different menu paths to reach configuration pages. For example, users who have a custom role with only intrusion policy privileges access the network analysis policy via the intrusion policy instead of the standard path through the access control policy.

For more information about user roles, see User Roles and Customize User Roles for the Web Interface.

---

**Firepower System IP Address Conventions**

You can use IPv4 Classless Inter-Domain Routing (CIDR) notation and the similar IPv6 prefix length notation to define address blocks in many places in the Firepower System.

When you use CIDR or prefix length notation to specify a block of IP addresses, the Firepower System uses **only** the portion of the network IP address specified by the mask or prefix length. For example, if you type 10.1.2.3/8, the Firepower System uses 10.0.0.0/8.

In other words, although Cisco recommends the standard method of using a network IP address on the bit boundary when using CIDR or prefix length notation, the Firepower System does not require it.

---

**Additional Resources**

The Firewalls Community is an exhaustive repository of reference material that complements our extensive documentation. This includes links to 3D models of our hardware, hardware configuration selector, product collateral, configuration examples, troubleshooting tech notes, training videos, lab and Cisco Live sessions, social media channels, Cisco Blogs and all the documentation published by the Technical Publications team.
Some of the individuals posting to community sites or video sharing sites, including the moderators, work for Cisco Systems. Opinions expressed on those sites and in any corresponding comments are the personal opinions of the original authors, not of Cisco. The content is provided for informational purposes only and is not meant to be an endorsement or representation by Cisco or any other party.

**Note**

Some of the videos, technical notes, and reference material in the Firewalls Community points to older versions of the Firepower Management Center. Your version of the Firepower Management Center and the version referenced in the videos or technical notes might have differences in the user interface that cause the procedures not to be identical.