



Getting Started With Firepower

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 7](#)
- [Search the FMC, on page 11](#)
- [Switching Domains on the Firepower Management Center, on page 18](#)
- [The Context Menu, on page 19](#)
- [Sharing Data with Cisco, on page 21](#)
- [Firepower Online Help, How To, and Documentation, on page 21](#)
- [Firepower System IP Address Conventions, on page 24](#)
- [Additional Resources, on page 24](#)
- [History for Getting Started with Firepower, on page 24](#)

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

Procedure

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

- **Firepower Management Center**

- *Cisco Firepower Management Center Getting Started Guide* for your hardware model, available from

<http://www.cisco.com/go/firepower-mc-install>

- **Firepower Threat Defense managed devices**

Important Ignore Firepower Device Manager documents on these pages.

- [Cisco Firepower 1010 Getting Started Guide](#)
- [Cisco Firepower 1100 Series Getting Started Guide](#)
- [Cisco Firepower 2100 Series Getting Started Guide](#)
- [Cisco Firepower 4100 Getting Started Guide](#)
- [Cisco Firepower 9300 Getting Started Guide](#)
- [Cisco Firepower Threat Defense for the ASA 5508-X and ASA 5516-X Using Firepower Management Center Quick Start Guide](#)
- [Cisco Firepower Threat Defense for the ISA 3000 Using Firepower Management Center Quick Start Guide](#)

- **Classic managed devices**

- [Cisco ASA FirePOWER Module Quick Start Guide](#)
-

Deploying Virtual Appliances

Follow these steps if your deployment includes virtual appliances. Use the documentation roadmap to locate the documents listed below: <http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html>.

Procedure

- 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 on the supported Public and Private cloud environment. See, [Cisco Secure Firewall Management Center Virtual Getting Started Guide](#).
- Step 3** Deploy virtual devices for your appliance on the supported Public and Private cloud environment. For details, see the following documentation.
- NGIPSv running on VMware: [Cisco Firepower NGIPSv Quick Start Guide for 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 Public and Private cloud environments, see [Cisco Secure Firewall Threat Defense Virtual Getting Started Guide, Version 7.3](#).
-

Logging In for the First Time

Before logging in to a new FMC for the first time, prepare the appliance as described in [Installing and Performing Initial Setup on Physical Appliances, on page 2](#) or [Deploying Virtual Appliances, on page 2](#).

The first time you log in to a new FMC (or an FMC newly restored to factory defaults), use the **admin** account for either the CLI or the web interface and follow the instructions in the *Cisco Firepower Management Center Getting Started Guide* for your FMC model. Once you complete the initial configuration process, the following aspects of your system will be configured:

- The passwords for the two **admin** accounts (one for web interface access and the other for CLI access) will be set to the same value, complying with strong password requirements as described in [Guidelines and Limitations for User Accounts](#). The system synchronizes the passwords for the two **admin** accounts only during the initial configuration process. If you change the password for either **admin** account thereafter, they will no longer be the same and the strong password requirement can be removed from the web interface **admin** account. (See [Add an Internal User at the Web Interface](#).)
- The following network settings the FMC uses for network communication through its management interface (eth0) will be set to default values or values you supply:
 - Fully qualified domain name (<hostname>.<domain>)
 - Boot protocol for IPv4 configuration (DHCP or Static/Manual)
 - IPv4 address
 - Network mask
 - Gateway
 - DNS Servers
 - NTP Servers

Values for these settings can be viewed and changed through the FMC web interface; see [Modify FMC Management Interfaces](#) and [Time and Time Synchronization](#) for more information.

- As a part of initial configuration the FMC configures a weekly automatic GeoDB update. You can observe the status of this update using the web interface Message Center. If configuring the update fails and your FMC has internet access, we recommend you configure regular GeoDB updates as described in [Schedule GeoDB Updates](#).
- As a part of initial configuration the FMC schedules a weekly task to download the latest software for the FMC and its managed devices. You can observe the status of this task using the web interface Message Center. If the task scheduling fails and your FMC has internet access, we recommend you schedule a recurring task for downloading software updates as described in [Automating Software Downloads](#).



Important This task only downloads software updates to the FMC. It is your responsibility to install any updates this task downloads. See the *Cisco Firepower Management Center Upgrade Guide* for more information.

- As a part of initial configuration the FMC schedules a weekly task to perform a locally-stored configuration-only backup. You can observe the status of this task using the web interface Message Center. If the task scheduling fails we recommend you schedule a recurring task to perform a backup as described in [Schedule FMC Backups](#).
- As a part of initial configuration the FMC downloads and installs the latest vulnerability database (VDB) update from the Cisco support site. This is a one-time operation. You can observe the status of this update using the web interface Message Center. To keep your system up to date, if your FMC has internet access, we recommend you schedule tasks to perform automatic recurring VDB update downloads and installations as described in [Vulnerability Database Update Automation](#).
- As a part of initial configuration the FMC configures a daily automatic intrusion rule update from the Cisco support site. (The FMC deploys automatic intrusion rule updates to affected managed devices when it next deploys affected policies.) You can observe the status of this update using the web interface Message Center. If configuring the update fails and your FMC has internet access, we recommend you configure regular intrusion rule updates as described in [Schedule Intrusion Rule Updates](#).

On completion of FMC initial configuration, the web interface displays the device management page, described in [Device Management Basics](#). (This is the default login page only for the first time the **admin** user logs in. On subsequent logins by the **admin** or any user, the default login page is determined as described in [Specifying Your Home Page](#).)

Once you have completed the initial configuration, 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 using the **admin** account for either the web interface or CLI and perform the initial configuration as described in the *Cisco Firepower Management Center Getting Started Guide* for your hardware model, available from <https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-guides-list.html>.

Procedure

- Step 1** Set a time zone for this account as described in [Setting Your Default Time Zone](#).
- Step 2** If needed, add licenses as described in [Licensing the Firepower System](#).
- Step 3** Add managed devices to your deployment as described in [Add a Device to the FMC](#).
- Step 4** Configure your managed devices as described in:
- [Introduction to IPS Device Deployment and Configuration](#), to configure passive or inline interfaces on Classic 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
- Step 5** 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 6** Apply the system-provided default health policy as described in [Applying Health Policies](#).
- Step 7** 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 [Configure an Access List](#).
 - 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 [Set the Language for the Web Interface](#).
 - If your organization restricts network access using a proxy server, edit your proxy settings as described in [Modify FMC Management Interfaces](#).
- Step 8** 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 9

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 create additional locally authenticated user accounts to access the FMC, see [Add an Internal User](#).
- If you want to use LDAP or RADIUS external authentication to allow access to the FMC, see [Configure External Authentication](#).

Step 10

Deploy configuration changes; see [Deploy Configuration Changes](#).

What to do next

- Review and consider configuring other features described in [Firepower Features, on page 7](#) 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:

- 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, 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](#).

End of Sale for Firepower 7000/8000 Series Devices

You cannot upgrade to or freshly install Firepower Version 6.5+ on 7000/8000 series devices. This guide and the related online help do not contain information on configuring or managing those devices.

If you are managing 7000/8000 series devices running supported *older* Firepower versions, use the following resources:

- For FMC-device compatibility, see the *About Firepower Management Centers* section in the [Cisco Firepower Compatibility Guide](#).
- For device configuration and management, see the [Firepower Management Center Configuration Guide](#) that corresponds to your device version.

Firepower Features

These tables list some commonly used Firepower features.

Appliance and System Management Features

To locate unfamiliar documents, see: <http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html>.

If you want to...	Configure...	As described in...
Manage user accounts for logging in to your Firepower appliances	Firepower authentication	User Accounts for FMC and User Accounts for Devices
Monitor the health of system hardware and software	Health monitoring policy	About Health Monitoring
Back up data on your appliance	Backup and restore	Backup and Restore
Upgrade to a new Firepower version	System updates	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 Firepower Release Notes
Baseline your physical appliance	Restore to factory defaults (reimage)	The Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 , for a list of links to instructions on performing fresh installations.

If you want to...	Configure...	As described in...
Update the VDB, intrusion rule updates, or GeoDB on your appliance	Vulnerability Database (VDB) updates, intrusion rule updates, or Geolocation Database (GeoDB) updates	System Updates
Apply licenses in order to take advantage of license-controlled functionality	Classic or Smart licensing	About Firepower Licenses
Ensure continuity of appliance operations	Managed device high availability and/or Firepower Management Center high availability	About Firepower Threat Defense High Availability About Firepower Management Center High Availability
Configure a device to route traffic between two or more interfaces	Routing	Routing Overview for Firepower Threat Defense
Configure packet switching between two or more networks	Device switching	Configure Bridge Group Interfaces
Translate private addresses into public addresses for internet connections	Network Address Translation (NAT)	Network Address Translation (NAT) for Firepower Threat Defense
Establish a secure tunnel between managed Firepower Threat Defense	Site-to-Site virtual private network (VPN)	VPN Overview for Firepower Threat Defense
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 <i>Firepower REST API Quick Start Guide</i>
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 configurations group multiple devices together as a single logical device, achieving increased throughput and redundancy.

Platform	High Availability	Clustering
Firepower Management Center	Yes	—
Firepower Management Center Virtual	Yes (See Virtual Platform Requirements for important details)	—

Platform	High Availability	Clustering
Firepower Threat Defense: <ul style="list-style-type: none"> • Firepower 1000 series • Firepower 2100 series • ASA 5500-X series • ISA 3000 	Yes	—
Firepower Threat Defense: <ul style="list-style-type: none"> • Firepower 4100/9300 chassis 	Yes	Yes
Firepower Threat Defense Virtual: <ul style="list-style-type: none"> • VMware • KVM 	Yes	—
Firepower Threat Defense Virtual (public cloud): <ul style="list-style-type: none"> • AWS • Azure 	—	—
NGIPSv	—	—
ASA FirePOWER	In these deployments, the ASA device provides the first-line system policy, then passes traffic to an ASA FirePOWER module for discovery and access control. See the ASA documentation for information on high availability and scalability configurations.	

Related Topics

[About Firepower Threat Defense High Availability](#)

[About Firepower Management Center High Availability](#)

Features for Detecting, Preventing, and Processing Potential Threats

To locate unfamiliar documents, see: <http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html>.

If you want to...	Configure...	As described in...
Inspect, log, and take action on network traffic	Access control policy, the parent of several other policies	Introduction to Access Control
Block or monitor connections to or from IP addresses, URLs, and/or domain names	Security Intelligence within your access control policy	About Security Intelligence

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

Integration with External Tools

To locate unfamiliar documents, see: <http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html>.

If you want to...	Configure...	As described in...
Automatically launch remediations when conditions on your network violate an associated policy	Remediations	Introduction to Remediations <i>Firepower System Remediation API Guide</i>

If you want to...	Configure...	As described in...
Stream event data from a Firepower Management Center to a custom-developed client application	eStreamer integration	eStreamer Server Streaming <i>Firepower System eStreamer Integration Guide</i>
Query database tables on a Firepower Management Center using a third-party client	External database access	External Database Access Settings <i>Firepower System Database Access Guide</i>
Augment discovery data by importing data from third-party sources	Host input	Host Input Data <i>Firepower System Host Input API Guide</i>
Investigate events using external event data storage tools and other data resources	Integration with external event analysis tools	Event Analysis Using External Tools
Troubleshoot issues	N/A	Troubleshooting the System

Search the FMC

You can use the global search feature to quickly locate and navigate to elements of your Firepower Management Center configuration.



Note This feature is supported in Light and Dusk themes only. To change the theme, see [Change the Web Interface Appearance](#).

You can search the FMC configuration for the following entities:

- Names of web interface pages in top-level menus. (See [Search for Web Interface Menu Options, on page 13.](#))
- For certain policy types:
 - Policy names
 - Policy descriptions
 - Rule names
 - Rule comments

(See [Search for Policies, on page 13.](#))

- For certain object types:
 - Object names
 - Object descriptions

- Configured values

(See [Search for Objects](#), on page 15 .)

Keep the following in mind when using global search:

- When you open the global search tool, the most recent ten searches appear in a history list below the search text box. You can select an item from this list to re-execute a search.
- When you type a search expression, the interface replaces the search history with search results that update as you type your search; you do not need to press Enter to execute the search.
- You can navigate the history list or the search results using the mouse or the keyboard arrow keys and the Enter key. Pressing the Enter key selects the currently highlighted item in the search results. In the case of results for web interface pages, this causes the FMC interface to display the highlighted page. For objects and policies, this displays details about the found entity.
- Search is not case-sensitive.
- In a multidomain deployment, search returns only objects and policies defined within the current domain.

For an object search, if your search expression is found in objects defined in domains other than your current default domain, the search results display the names of the domains within which those objects reside. If your search expression is found in objects defined within your current domain, the search results display the object values.

- You can use the following wildcard characters in your search:
 - ? matches any single character.
 - * matches any 0 or more characters.
 - ^ anchors the search term it precedes to the beginning of matched entities.
 - \$ anchors the search term it follows to the end of matched entities

Wildcards cannot be escaped.

- For greater efficiency, global search does not return indirect search results; that is, global search does not return policies or objects that reference objects where a search term is found. However, you can determine which policies or objects reference many found objects by viewing the **Usages** tab for the found object in the search detail pane.
- Global search returns the top results for your search expression determined by its relevance to the most commonly used configuration entities in the FMC. If global search fails to return something you are expecting to find, try refining your search, try using the search or filter tool that appears at the top of many GUI pages, or try some of the configuration-specific search features the web interface offers:
 - [Searching for Rules](#)
 - [Searching and Filtering the NAT Rule Table](#)
 - [Searching TLS/SSL Rules](#)
 - [Searching for Events](#)
 - [Searching Custom Tables](#)


Search for Web Interface Menu Options

You can search to find locations of pages in the top-level menus of the web interface. For example, to view or configure Quality of Service settings, search for **QoS**.

Before you begin

This feature is not available in the Classic theme. To change the theme, see [Change the Web Interface Appearance](#).

Procedure

-
- Step 1** Use one of two methods to initiate a search:
- In the menu bar at the top of the Firepower Management Center web interface, click **Search** .
 - With focus outside of a text box, type / (forward slash).
- Step 2** Enter one or more letters of the name of the menu option you seek. Search results appear below the text box and update as you type; you do not need to press Enter to execute the search.
- Step 3** Search results appear grouped by category. To go to a page listed under **Navigation**, click the menu path in the search results list.
-

Search for Policies

The following table indicates which policy types you can search for by name:

In Scope	Out of Scope
Access Control Policy	Threat Defense Platform Settings
Prefilter Policy	Firepower Settings Policy
Threat Defense NAT Policy	Firepower NAT Policy
Intrusion category	QoS Policy
• Intrusion Policy	FlexConfig Policy
• Network Analysis Policy	
	DNS Policy
	Malware & File Policy
	SSL Policy
	Identity Policy
	Network Discovery

In Scope	Out of Scope
	Application Detector Correlation Policy VPN category <ul style="list-style-type: none"> • Dynamic Access Policy • Site To Site • Remote Access

Global search returns policies whose names match the search term, as well as access control policies using rules whose name or comments match the search term. If you see an access control policy in the search result list whose name does not match the search, the match was made on the name or comments for a rule configured within the policy.



Important Global search returns the top results for your search expression determined by its relevance to the most commonly used configuration entities in the FMC. Your search term may exist in policy types that are not in scope for this search feature. For a full description of the global search feature and alternative search methods, see [Search the FMC](#).


Before you begin

This feature is not available in the Classic theme. To change the theme, see [Change the Web Interface Appearance](#).

Procedure

- Step 1** Use one of two methods to initiate a search:
- In the menu bar at the top of the Firepower Management Center web interface, click **Search** (🔍).
 - With focus outside of a text box, type / (forward slash).
- Step 2** Enter a search expression in the search text box. Search results appear below the text box and update as you type; you do not need to press Enter to execute the search.
- Step 3** Search results appear grouped by category. Under the **Policies** category you can do the following:

To:	Do this:
View search results for a single policy type.	Click the policy type in the search results, such as Access Control Policy.
View details about a policy.	Click the policy name in the search results list to view the details pane and display the General tab.

To:	Do this:
View the Access Control policies that reference Intrusion and Network Analysis policies.	Click the name of the Intrusion or Network Analysis policy in the search results to view the details pane and display the Usages tab.
Open the policy configuration page for a policy in a separate browser window.	Click the policy name in the search results, and in the details pane click Edit ().

Search for Objects

The following table indicates which object types listed on the Object Management page (**Objects > Object Management**) are in scope for the Global Search feature:

In Scope	Out of Scope
AAA Server category <ul style="list-style-type: none"> • RADIUS Server Group • Single Sign-On Server 	Application Filters Cipher Suite List Community List
Access List category <ul style="list-style-type: none"> • Extended Access List • Standard Access List 	Distinguished Name category <ul style="list-style-type: none"> • Individual Distinguished Name Objects • Distinguished Name Object Groups
Address Pools category <ul style="list-style-type: none"> • IPv4 Pools • IPv6 Pools 	File List FlexConfig category <ul style="list-style-type: none"> • FlexConfig Object • Text Object
AS Path	

In Scope	Out of Scope
<p>DNS Server Group</p> <p>External Attributes Category</p> <ul style="list-style-type: none"> • Dynamic Object • Security Group Tag <p>Geolocation</p> <p>Interface category</p> <ul style="list-style-type: none"> • Security Zone • Interface Group <p>Key Chain</p> <p>Network (includes Network, Host, Range, FQDN, Network Group)</p> <p>PKI category</p> <ul style="list-style-type: none"> • Cert Enrollment <p>Policy List</p> <p>Port (objects and groups, TCP, UDP, ICMP, ICMPv6, other)</p> <p>Prefix List category</p> <ul style="list-style-type: none"> • IPv4 Prefix List • IPv6 Prefix List <p>Route Map</p> <p>SLA Monitor</p> <p>Time Range</p> <p>Time Zone</p> <p>Tunnel Zone</p> <p>URL (Objects, groups.)</p> <p>VLAN Tag (Objects, groups.)</p>	<p>PKI category</p> <ul style="list-style-type: none"> • External Cert Groups • External Certs • Internal CA Groups • Internal CAs • Internal Cert Groups • Internal Certs • Trusted CA Groups • Trusted CAs <p>Security Intelligence category</p> <ul style="list-style-type: none"> • DNS Lists and Feeds • Network Lists and Feeds • URL Lists and Feeds <p>Sinkhole</p> <p>Variable Set</p> <p>VPN category</p> <ul style="list-style-type: none"> • AnyConnect File • Custom Attribute

In Scope	Out of Scope
VPN category <ul style="list-style-type: none"> • Certificate Map • Group Policy • IKEv1 IPsec Proposal • IKEv1 Policy • IKEv2 IPsec Proposal • IKEv2 Policy 	

Global search returns objects whose names or description match the search term, as well as objects with configured values that match the search term. If you see an object in the search result list whose name does not match the search, the match was made on the description or a configured value within the object.



Important

Global search returns the top results for your search expression determined by its relevance to the most commonly used configuration entities in the FMC. Your search term may exist in object types that are not in scope for this search feature. For a full description of the global search feature and alternative search methods, see [Search the FMC](#).

Object searches can be particularly useful when you need to locate network information within your deployment. You can search for the following in object names, descriptions, or configured values:

- IPv4 and IPv6 address information, including the following formats:
 - Full addresses (For example, 194.164.0.23, 2001:0db8:85a3:0000:0000:8a2e:0370:7334.)
 - Partial addresses (For example, 194.164, 2001:db8.)
 - Ranges (For example, 192.164.1.1-192.168.1.5 or 2001:db8::0202-2001:db8::8329. Do not add a space before or after the hyphen.) Global search returns objects using network addresses that match any within the specified range.
 - CIDR notation. (For example 192.168.1.0/24, 2002::1234:abcd:ffff:101/64.) Global search returns objects using network addresses that match any within the specified CIDR block.
- Port information:
 - Port numbers (For example, 22 or 80.)
 - Protocols. (For example, https or ssh.)
- Fully qualified domain names. (For example, www.cisco.com.)
- URLs. (For example, http://www.cisco.com.)
- Encryption standards or hash types. (For example, AES-128 or SHA.)
- VLAN tag numbers. (For example, 568.)

Before you begin

This feature is not available in the Classic theme. To change the theme, see [Change the Web Interface Appearance](#).

Procedure**Step 1**

Use one of two methods to initiate a search:

- In the menu bar at the top of the Firepower Management Center web interface, click **Search** (🔍).
- With focus outside of a text box, type / (forward slash).

Step 2

Enter a search expression in the search text box. Search results appear below the text box and update as you type; you do not need to press Enter to execute the search.

If your search expression is found in objects defined in domains other than your current default domain, the search results display the names of the domains within which those objects reside. If your search expression is found in objects defined within your current domain, the search results display the object values.

Step 3

Search results appear divided by category. Under the **Object** category you can do the following:

To:	Do this:
View search results for a single object type.	Click on the object type in the search results, such as Network .
View details about an object in the search results.	Click the object name in the search results to view the details pane and display the General tab.
View a list of policies or objects that use an object in the search results.	Click the object name in the search results to view the details pane and display the Usages tab. Note Global Search does not provide usage information for all object types.
Open the object configuration page for an object in the search results in a separate browser window.	Click the object name in the search results, and in the details pane click Edit (✎).

Switching Domains on the Firepower Management Center

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.

Procedure

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](#).

While viewing connection events, you can add items to the default Security Intelligence Block and Do Not Block lists:

- 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** > **Page-Level Help**

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 uncheck the **Enable How-Tos** check box in **How-To Settings**.



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.

For the list of walkthroughs available on FMC, see [Feature Walkthroughs Supported on Firepower Management Center](#).

You can find additional documentation related to the Firepower system using the documentation roadmap: <http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html>.

Top-Level Documentation Listing Pages for FMC Deployments

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



Note 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 FMC. 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:
<http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html>
- Firepower Management Center Virtual appliances:
 - <http://www.cisco.com/c/en/us/support/security/defense-center-virtual-appliance/tsd-products-support-series-home.html>
 - <http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html>

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

- Firepower Threat Defense software:
<http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html>
- Firepower Threat Defense Virtual:
<http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/tsd-products-support-series-home.html>
- Firepower 1000 series:
<https://www.cisco.com/c/en/us/support/security/firepower-1000-series/tsd-products-support-series-home.html>
- Firepower 2100 series:
<https://www.cisco.com/c/en/us/support/security/firepower-2100-series/tsd-products-support-series-home.html>
- Firepower 4100 series:
<https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html>
- Firepower 9300:
<https://www.cisco.com/c/en/us/support/security/firepower-9000-series/tsd-products-support-series-home.html>
- ISA 3000:
<https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html>

Classic devices, also called NGIPS (Next Generation Intrusion Prevention System) devices

- ASA with FirePOWER Services:
 - ASA 5500-X with FirePOWER Services:
 - <https://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html>
 - <https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html>
 - ISA 3000 with FirePOWER Services:
<https://www.cisco.com/c/en/us/support/security/industrial-security-appliance-isa/tsd-products-support-series-home.html>
- NGIPSv (virtual device):
<https://www.cisco.com/c/en/us/support/security/ngips-virtual-appliance/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, many features are supported only on Firepower Threat Defense 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 FMC. Your version of the FMC 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.

History for Getting Started with Firepower

Feature	Version	Details
Search for certain policies and objects	7.0	<p>You can search for certain policies by name and for certain objects by name and configured value.</p> <p>For specifics, see Search for Policies, on page 13 and Search for Objects, on page 15.</p> <p>This feature uses the existing Search button at the top of the FMC web interface window.</p> <p>Platform: FMC (not available when using the Classic theme)</p>

Feature	Version	Details
Search for web interface pages	6.7	<p>You can search for pages you want to view or change. For example, you can search for QoS to locate the page to configure Quality of Service settings.</p> <p>New/Modified Screens: There is a new magnifying glass button at top of the FMC web interface window.</p> <p>Platform: FMC (not available when using the Classic theme)</p>
Initial Configuration Wizard	6.5	<p>Initial login on a new or newly-restored-to-factory-defaults FMC now presents the admin user with an Initial Configuration Wizard documented in the <i>Cisco Firepower Management Center Getting Started Guide</i> for FMC models that support Version 6.5. The wizard configures the following:</p> <ul style="list-style-type: none"> • The passwords for the two admin accounts (one for web interface access and the other for CLI access) are set to the same value, complying with strong password requirements. • The network settings the FMC uses for network communication through its management interface (eth0) are established. • Weekly automatic updates for the GeoDB and system software for the FMC and its managed devices are scheduled. • Weekly locally-stored configuration-only automatic backups for the FMC are scheduled. <p>New/Modified Screens:</p> <p>Initial login for admin user</p> <p>Supported Platforms: FMC</p>

