

Firewall Management Center overview

The Firewall Management Center is a powerful web-based multi-device manager that runs on its own server hardware or as a virtual device on a hypervisor. Use the Firewall Management Center if you want a multi-device manager and require all features on the Firewall Threat Defense. The Firewall Management Center also provides powerful analysis and monitoring of traffic and events.

The Firewall Management Center is not compatible with other managers because the Firewall Management Center owns the Firewall Threat Defense configuration. Configure the Firewall Threat Defense using the Firewall Management Center. Direct configuration is not supported.

- Quick start basic setup, on page 1
- Unsupported screens for the latest device version, on page 6
- Firewall Threat Defense devices, on page 7
- Firepower Features, on page 7
- Global search features in Firewall Management Center, on page 11
- Switch domains on Secure Firewall Management Center, on page 22
- Context menus, on page 23
- Data sharing features with Cisco, on page 24
- Online help and documentation, on page 25
- IP address conventions, on page 27
- Additional Resources, on page 27

Quick start basic setup

Quick start basic setup is a configuration approach that enables rapid deployment of Firepower feature sets and managed devices to begin controlling and analyzing network traffic with minimal initial configuration effort.

Setup capabilities

The Firepower feature set provides powerful and flexible capabilities that support both basic and advanced configurations for Secure Firewall Management Center and its managed devices.

Installing and performing initial setup on physical appliances

Procedure

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

- **Firewall Management Center**
  - Secure Firewall Threat Defense: install and upgrade guides for your hardware model, available from

    https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-guides-list.htmlhttp://www.cisco.com/go/firepower-mc-install
- **Firewall Threat Defense managed devices**
  - Firepower 1010 getting started guides
  - Firepower 1100 getting started guides
  - *Cisco Firepower 2100 Getting Started Guide*
  - Cisco Secure Firewall 3100 Getting Started Guide
  - *Cisco Firepower 4100 Getting Started Guide*
  - *Cisco Firepower 9300 Getting Started Guide*
  - Cisco Firepower Threat Defense for the ISA 3000 Using Firepower Management Center Quick Start Guide

Deploy virtual appliances

This task enables you to deploy virtual appliances for Cisco Secure Firewall by identifying supported platforms and using the correct deployment guides for Management Centers and devices.

Deploy virtual appliances when your network architecture requires virtualized Cisco Secure Firewall Management Centers or devices, such as in cloud or virtualized environments.

Use the documentation roadmap to locate the relevant deployment guides: https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.htmlhttp://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html. Follow these steps if your deployment includes virtual appliances.

Before you begin

Review your deployment requirements. Ensure you have access to the compatibility guide and the appropriate deployment documentation for your environment. Determine whether you are deploying Management Centers, devices, or both as virtual appliances. Follow these steps to deploy virtual appliances:

Procedure

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

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

- Firewall Management Center Virtual running on VMware: *Cisco Secure Firewall Management Center Virtual Getting Started Guide*
- Firewall Management Center Virtual running on AWS: *Cisco Secure Firewall Management Center Virtual Getting Started Guide*
- Firewall Management Center Virtual running on KVM: *Cisco Secure Firewall Management Center Virtual Getting Started Guide*

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

- Firewall Threat Defense Virtual running on VMware: *Cisco Secure Firewall Threat Defense Virtual for VMware Getting Started Guide*
- Firewall Threat Defense Virtual running on AWS: *Cisco Secure Firewall Threat Defense Virtual for AWS Getting Started Guide*
- Firewall Threat Defense Virtual running on KVM: *Cisco Secure Firewall Threat Defense Virtual for KVM Getting Started Guide*
- Firewall Threat Defense Virtual running on Azure: *Cisco Secure Firewall Threat Defense Virtual for Azure Getting Started Guide*

After you complete these steps, your virtual appliances are deployed. Configure and integrate them into your network environment.

What to do next

- Refer to the configuration guides for further setup and integration of your deployed virtual appliances.
- Verify connectivity and functionality of the Management Centers and devices.

First-time login

A first-time login is a system access event that

- requires preparation of the appliance as described in Installing and performing initial setup on physical appliances, on page 2 or Deploy virtual appliances, on page 2.
- uses the **admin** account for CLI access or web interface access and refers to the instructions in the *Cisco Secure Firewall Management Center Getting Started Guide* for the specific model, and
- completes initial configuration, setting system aspects such as passwords, network settings, and enabling telemetry features.

Initial configuration settings

These aspects of your system are configured during the first login:

- During initial configuration, the system sets the passwords for the two **admin** accounts (web interface and CLI) to the same value. This process enforces strong password requirements as described in Guidelines and limitations for user accounts for Firewall Management Center. The system synchronizes the passwords only during initial configuration. If you later change the password for either account, the passwords will no longer match, and the web interface **admin** account will no longer require a strong password. (Refer to Add or edit an internal user.)
- During the first login, you must configure network settings for the Firewall Management Center. These settings determine how the system communicates through its management interface (eth0). By default, values are supplied, but you can set custom values as needed:
  - Fully qualified domain name (`<hostname>.<domain>`)
  - Boot protocol for IPv4 configuration (DHCP or Static Manual)
  - IPv4 address
  - Subnet mask
  - Gateway
  - DNS servers
  - NTP servers

  You can view and change these settings through the Firewall Management Center web interface. For more information, refer to Modify Firewall Management Center management interfaces and Time synchronization.
- As part of the initial configuration, the system schedules multiple update-related tasks. We recommend you review these tasks to make sure they run at the right time for your environment:
  - Daily intrusion rule updates. Refer to Schedule intrusion rule updates.
  - Weekly geolocation database (GeoDB) updates. Refer to Schedule GeoDB updates.
  - Weekly maintenance release, patch, and vulnerability database (VDB) downloads. Refer to Scheduling.
- As part of the initial configuration, the system downloads and installs the latest VDB. To keep the system up to date, schedule recurring updates. Refer to Scheduling.

After you complete the Firewall Management Center initial configuration, the web interface displays the device management page described in *Cisco Secure Firewall Management Center Device Configuration Guide*.

(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 Specify your home page.)

After you complete the initial configuration, you can begin controlling and analyzing traffic by configuring basic policies. For details, refer to Configure basic policies and settings, on page 5.

Configure basic policies and settings

This task guides you to configure and deploy basic policies and system settings, so you can begin to monitor and manage your deployment effectively.

- Establishes initial access and configuration for your system.
- Ensures that essential policies are in place for data visibility and system operation.

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

This guide does not provide a comprehensive discussion of policy or feature capabilities. For information about additional features and advanced configurations, refer to other sections in this guide.

Before you begin

Log in to the web interface using the **admin** account for web interface or CLI. Perform the initial configuration as described in the *Cisco Secure Firewall Management Center Getting Started Guide*, which is available for your hardware model from the Install and Upgrade Guides.

Follow these steps to configure basic policies and settings:

Procedure

Step 1 Set a time zone for this account as described in Set your default time zone.

Step 2 If needed, add licenses as described in Licenses.

Step 3 Add managed devices to your deployment. For detailed instructions, refer to *Add a Device to the Firewall Management Center* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Step 4 Configure your managed devices as described in:

- *Interface Overview* in the *Cisco Secure Firewall Management Center Device Configuration Guide*, to configure transparent or routed mode on Firewall Threat Defense devices.
- *Interface Overview* in the *Cisco Secure Firewall Management Center Device Configuration Guide*, to configure interfaces on the Firewall Threat Defense devices.

Step 5 Configure an access control policy as described in *Creating a Basic Access Control Policy* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

- Set the **Balanced Security and Connectivity** intrusion policy as your default action in most cases. For more information, refer to *Access Control Policy Default Action* and *System-Provided Network Analysis and Intrusion Policies* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- 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, refer to Connection logging.

Step 6 Apply the system-provided default health policy as described in Apply a health policy.

Step 7 Customize a few of your system configuration settings:

- To allow inbound connections for a service such as SNMP or syslog, modify the relevant ports in the access list. For detailed instructions, refer to Configure an access list.
- Edit your database event limits if needed. For additional information, refer to Configure database event limits.
- To change the display language, edit the language setting as described in Set the language for the web interface.
- To use a proxy server for restricted network access, edit your proxy settings as described in Modify Firewall Management Center management interfaces.

Step 8 Customize your network discovery policy as described in *Configuring the Network Discovery Policy* in the *Cisco Secure Firewall Management Center Device Configuration Guide*. By default, the network discovery policy analyzes all network traffic. Limit discovery to RFC 1918 addresses in most cases.

Step 9 Consider customizing these other common settings:

- If you want to customize the default values for system variables, understand their use as described in *Variable Sets* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- If you want to create additional locally authenticated user accounts to access the Firewall Management Center, refer to Add or edit an internal user.
- To allow access to the Firewall Management Center through LDAP or RADIUS external authentication, refer to External authentication configuration for Firewall Management Center.

Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

After you complete these steps, your system allows you to view data in dashboards and event tables and proceed with more feature customization if needed.

What to do next

Review and consider configuring other features described in Firepower Features, on page 7 and the rest of this guide.

Unsupported screens for the latest device version

You have reached this help page because the Firewall Management Center screen is a deprecated feature and is not supported on the latest version of device software.

- This guide includes features supported on the latest version of device software. Although the Firewall Management Center can manage devices running previous versions (as specified in the compatibility matrix available at *Cisco Secure Firewall Threat Defense Compatibility Guide*), refer to the appropriate guide for features supported only on older versions.
- Refer to the guide that matches your device version for features that are supported only on older device versions. Use the on-prem guide for other versions, as

Firewall Threat Defense devices

A Firewall Threat Defense device is a next-generation firewall (NGFW) that

- provides NGIPS capabilities
- supports site-to-site and remote access VPN, robust routing, NAT, clustering, and application inspection, and
- is available on a wide range of physical and virtual platforms.

Manager-device compatibility

This section explains compatibility between managers and devices, covering software, device models, virtual hosting environments, and operating systems.

Refer to the Release Notes for Secure Firewall Threat Defense, *Cisco Secure Firewall Management Center Compatibility Guide*, and *Cisco Secure Firewall Threat Defense Compatibility Guide* for more information.

Typical deployment scenario

In a typical deployment, multiple traffic-handling devices report to one Secure Firewall Management Center, which is used for administrative, management, analysis, and reporting tasks.

Firepower Features

The tables present commonly used Firepower features.

Understand appliance and system management features

To locate documents, refer to: Navigating the Cisco Secure Firewall Threat Defense Documentation.

This reference lists the main features for managing appliances and systems, such as user accounts, device health, backup and restore, upgrades, licensing, high availability, routing, VPN, multitenancy, REST API access, and troubleshooting.

Table 1: Appliance and system management features

If you want to...	Configure...	As described in...
Manage user accounts for logging in to your Secure Firewall devices	Device authentication	Users and *Users for Devices* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Monitor the health of system hardware and software	Health monitoring policy	Health monitoring
Back up data on your appliance	Backup and restore	Backup/Restore

If you want to...	Configure...	As described in...
Upgrade to a new version	System updates	Secure Firewall Threat Defense upgrade guides for Firewall Management Center Release Notes for Secure Firewall Threat Defense
Baseline your physical appliance	Restore to factory defaults (reimage)	Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Threat Defense *Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense*
Update the VDB, intrusion rule updates, or GeoDB on your appliance	Vulnerability Database (VDB) updates, intrusion rule updates, or Geolocation Database (GeoDB) updates	Updates
Apply licenses in order to take advantage of license-controlled functionality	Smart licensing	Licenses
Ensure continuity of appliance operations	Managed device high availability and/or Firewall Management Center high availability	*About Secure Firewall Threat Defense "High Availability chapter"* in the *Cisco Secure Firewall Management Center Device Configuration Guide* High availability in Firewall Management Center
Configure a device to route traffic between two or more interfaces	Routing	*Reference for Routing* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Configure packet switching between two or more networks	Device switching	*Configure Bridge Group Interfaces* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Translate private addresses into public addresses for internet connections	Network Address Translation (NAT)	*Network Address Translation* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Establish a secure tunnel between managed Firewall Threat Defense devices	Site-to-Site virtual private network (VPN)	*VPN Overview* in the *Cisco Secure Firewall Management Center Device Configuration Guide*

If you want to...	Configure...	As described in...
Establish secure tunnels between remote users and managed Firewall Threat Defense devices	Remote Access VPN	*VPN Overview* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Segment user access to managed devices, configurations, and events	Multitenancy using domains	Multitenancy using domains
View and manage appliance configuration using a REST API client	REST API and REST API Explorer	REST API preferences *Secure Firewall Mangement Center REST API Quick Start Guide*
Troubleshoot issues	N/A	Troubleshooting

Use features to detect, prevent, and process potential threats

To locate documents, refer to: Navigating the Cisco Secure Firewall Threat Defense Documentation.

This reference lists the features and policies you can use to detect, prevent, and process potential threats on your network, along with links to configuration topics and guides.

Table 2: Features for detecting, preventing, and processing potential threats

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	*Access Control Policy* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Block or monitor connections to or from IP addresses, URLs, or domain names, or both	Security Intelligence within your access control policy	*About Security Intelligence* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Control the websites that users on your network can access	URL filtering within your policy rules	*URL Filtering* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Monitor malicious traffic and intrusions on your network	Intrusion policy	*Intrusion Policy Basics* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Block encrypted traffic without inspection Inspect encrypted or decrypted traffic	SSL policy	*SSL Policies Overview* in the *Cisco Secure Firewall Management Center Device Configuration Guide*

If you want to...	Configure...	As described in...
Tailor deep inspection to encapsulated traffic and improve performance with fastpathing	Prefilter policy	*About Prefiltering* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Rate limit network traffic that is allowed or trusted by access control	Quality of Service (QoS) policy	*About QoS Policies* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Allow or block files (including malware) on your network	File/malware policy	*Network Malware Protection and File Policies* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Operationalize data from threat intelligence sources	Cisco Threat Intelligence Director (TID)	*Threat Intelligence Director Overview* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Configure passive or active user authentication to perform user awareness and user control	User awareness, user identity, identity policies	*About User Identity Sources* in the *Cisco Secure Firewall Management Center Device Configuration Guide* *About Identity Policies* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Collect host, application, and user data from traffic on your network to perform user awareness	Network Discovery policies	*Network Discovery Policies* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Use tools beyond your device 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	*Application Detection* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
Troubleshoot issues	N/A	Troubleshooting

Integrate with external tools

This reference describes how to integrate with external tools for automation, event streaming, database access, host input, event analysis, and troubleshooting in your network environment.

Table 3: Integration options with external tools

If you want to...	Configure...	As described in...
Automatically launch remediations when conditions on your network violate an associated policy	Remediations	Introduction to remediations *Firepower System Remediation API Guide*
Stream event data from a Firewall Management Center to a custom-developed client application	eStreamer integration	eStreamer server streaming *Secure Firewall Mangement Center Event Streamer Integration Guide*
Query database tables on a Firewall Management Center using a third-party client	External database access	External database access *Secure Firewall Mangement Center Database Access Guide*
Augment discovery data by importing data from third-party sources	Host input	*Host Input Data* in the *Cisco Secure Firewall Management Center Device Configuration Guide* *Firepower System Host Input API Guide*
Investigate events with external event data storage tools and additional resources.	Integration with external event analysis tools	Event Analysis Using External Tools
Troubleshoot issues	N/A	Troubleshooting

Global search features in Firewall Management Center

A global search feature is a configuration navigation tool that

- enables users to quickly locate and access elements within the Firewall Management Center configuration
- supports searching for web interface pages, policy types, object types, and walkthroughs,
- provides search history, wildcard support, and results based on relevance.

Global search configuration entities

You can search the Firewall Management Center configuration for these entities:

- Names of web interface pages in top-level menus. (Refer to Search for web interface menu options, on page 15)
- For certain policy types:
  - Policy names
  - Policy descriptions
  - Rule names
  - Rule comments

  (Refer to Search for policies, on page 15)
- For certain object types:
  - Object names
  - Object descriptions
  - Configured values

  (Refer to Search for Objects, on page 17)
- How To walkthroughs.

  The search returns a list of walkthroughs that contain the search term, with links to each. (Refer to Search for how to walkthroughs, on page 21)

Global search usage details:

- When you open the global search tool, the ten most recent searches appear in a history list below the search text box. You can select an item from this list to repeat a search.
- When you type a search expression, the system updates the search results and replaces the search history. You do not need to press Enter to execute the search.
- Navigate the history list or search results using the mouse, keyboard arrow keys, or the Enter key. Press Enter to select the highlighted item in the search results. For web interface pages, the Firewall Management Center interface displays the highlighted page. For objects and policies, the interface displays details about the found entity.
- Search is not case-sensitive.
- You can use these 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. It does not return policies or objects referencing those with the search term. To see which policies or objects reference found items, view the **Usages** tab 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 Firewall Management Center. If global search does not return a result you expect, try refining your search. You can also use the search or filter tool at the top of many GUI pages, or explore configuration-specific search features that the web interface offers:
  - *Searching for Rules* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
  - *Searching and Filtering the NAT Rule Table* in the *Cisco Secure Firewall Management Center Device Configuration Guide*
  - Searching for Events
  - Searching Custom Tables



Note This feature is supported in Light and Dusk themes only. To change the theme, refer to Change the web interface appearance.

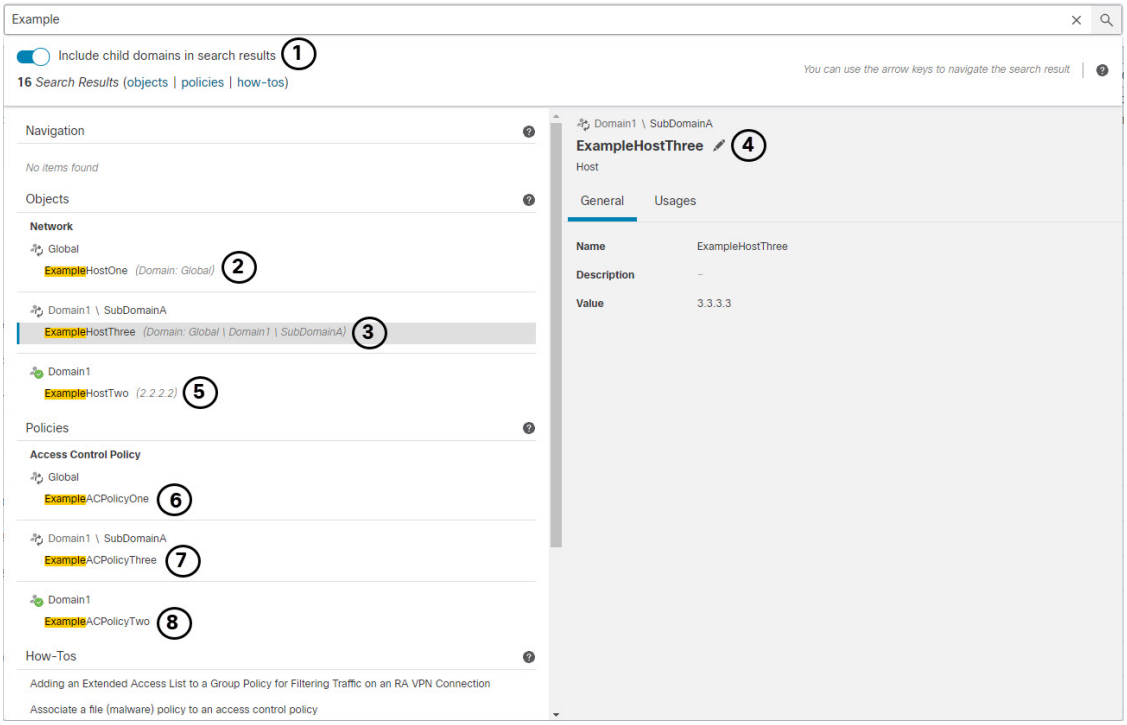
Global search in a multidomain deployment

In a multidomain deployment, by default search returns only objects and policies defined within the current domain and its ancestor domains. You can view objects and policies in child domains by toggling an option in the search results dialog.

For an object search, if your search expression is found in objects defined in domains other than your current 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.

The screenshot demonstrates a deployment with three domains at three levels: Global, Domain1, and SubDomainA. The user, with Domain1 as the current domain, has entered a search for the string “example” in both ancestor and child domains.

Figure 1: Example of global search in a multidomain environment



1	The user has chosen to search child domains (SubDomainA) as well as the current domain (Domain1) and its ancestor (Global).	2	A matching network object ExampleHostOne defined in the parent domain Global is displayed with the domain name, and the **External Domain** ( ) icon indicating the user must switch domains to edit details.
3	The matching network object ExampleHostThree defined in the child domain SubDomainA is displayed with the domain name, and the **External Domain** ( ) icon indicating the user must switch domains to edit details. This object is currently selected.	4	The matching network object ExampleHostThree is currently selected, and information is provided in the right pane. The **External Domain** ( ) icon indicates that when the user clicks **Edit** ( ), the system will prompt the user to confirm a domain change before allowing edit access to the object.
5	The matching network object ExampleHostTwo, defined in the current domain, is displayed with the object value, and with the **Current Domain** ( ) icon indicating the user may edit this object without switching domains.	6	The matching access control policy ExampleACPolicyOne defined in the parent domain Global is displayed with the domain name, and the **External Domain** ( ) icon indicating the user must switch domains to edit details.

7	The matching access control policy ExampleACPolicyThree defined in the child domain SubDomainA is displayed with the domain name, and the **External Domain** ( ) icon indicating the user must switch domains to edit details.	8	The matching access control policy ExampleACPolicyTwo defined in the current domain is displayed with the **Current Domain** ( ) icon indicating the user may edit details without switching domains.

Search for web interface menu options

Search in the Secure Firewall Management Center web interface to quickly find menu options and pages. Use the search function to navigate efficiently and access configuration pages.

Search the top-level menus in the web interface to locate the pages you need.

To view or configure Quality of Service settings, search for `QoS`. The search results update as you type and are grouped by category.

Before you begin

This feature is unavailable in the Classic theme. To change the theme, refer to Change the web interface appearance. Ensure you use a supported theme for search functionality.

Follow these steps to search for web interface menu options:

Procedure

Step 1 Use one of the two methods to initiate a search:

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

Step 2 Enter one or more letters of the menu option's name. The search results appear and update as you type. You do not need to press Enter.

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.

After completing these steps, you can access desired pages or menu options in the Secure Firewall Management Center web interface. The search results display in groups by category, which allows efficient navigation.

Search for policies

Configure global search to efficiently locate policies by name or rule comments in the web interface. This task helps you find policy types and their details so you can streamline policy management and review.

You can search for specific policy types by name using global search. This table shows which policy types are in scope for search and which are not:

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 • Intrusion Policy • Network Analysis Policy	QoS Policy FlexConfig Policy DNS Policy Malware and File Policy SSL Policy Identity Policy Network Discovery Application Detector Correlation Policy VPN category • 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 view an access control policy in the search result list whose name does not match your search, the match occurs because the name or comments for a rule configured within the policy matched your search term.

- Global search returns the top results for your search expression determined by its relevance to the most commonly used configuration entities in the Firewall Management Center.
- 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, refer to Search the Firewall Management Center.

Before you begin

This feature is not available in the Classic theme. To change the theme, refer to Change the web interface appearance.

Follow these steps to search for policies using global search:

Procedure

Step 1 Use one of the two methods to initiate a search:

- In the menu bar at the top of the Firewall 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 are displayed under the text box and update as you type. You do not need to press Enter to execute the search.

Step 3 (Optional) In a multidomain deployment, if your current domain has descendant domains, you can toggle **Include child domains in search results** to view policies in those descendant domains.

Step 4 Search results appear grouped by category. In a multidomain deployment, within the **Policies** category the search results are grouped by the domains within which found policies are defined. Under the **Policies** category, you can:

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.
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. In the details pane, click the **Edit** ( ). In a multidomain deployment, if you choose to edit a policy not defined within your current domain the system will prompt you to change your current domain.

After completing these steps, you will be able to locate and access policies and their details using global search. Search results are grouped by category and domain, allowing for efficient policy management.

Search for Objects

This 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 • RADIUS Server Group • Single Sign-On Server Access List category • Extended Access List • Standard Access List Address Pools category • IPv4 Pools • IPv6 Pools AS Path Community List category • Extended Community DNS Server Group External Attributes Category • Dynamic Object • Security Group Tag Geolocation Interface category • Security Zone • Interface Group Key Chain Network (includes Network, Host, Range, FQDN, Network Group) PKI category Cert Enrollment Policy List Port (objects and groups, TCP, UDP, ICMP, ICMP6, other)	Application Filters Cipher Suite List Community List Category • Community Distinguished Name category • Individual Distinguished Name Objects • Distinguished Name Object Groups File List FlexConfig category • FlexConfig Object • Text Object PKI category • External Cert Groups • External Certs • Internal CA Groups • Internal CAs • Internal Cert Groups • Internal Certs • Trusted CA Groups • Trusted CAs Security Intelligence category • DNS Lists and Feeds • Network Lists and Feeds • URL Lists and Feeds Sinkhole Variable Set

In Scope	Out of Scope
Prefix List category • IPV4 Prefix List • IPV6 Prefix List Route Map SLA Monitor Time Range Time Zone Tunnel Zone URL (Objects, groups) VLAN Tag (Objects, groups) VPN category • Certificate Map • Group Policy • IKEv1 IPsec Proposal • IKEv1 Policy • IKEv2 IPSec Proposal • IKEv2 Policy	VPN category • AnyConnect File • Custom Attribute

Global search shows objects whose names, descriptions, or configured values match your search term. If you find an object in the results and its name does not match your search, the match comes from the description or another configured value.



Important Global search returns the top results for your search expression, based on relevance to the most commonly used configuration entities in the Firewall Management Center. 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, refer to Search the Firewall Management Center .

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

- IPv4 and IPv6 address information, including these 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, refer to 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 Firewall 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 are shown in the text box and update as you type. There is no 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 (Optional) In a multidomain deployment, if your current domain has descendant domains, you can toggle **Include child domains in search results** to view objects in those descendant domains.

Step 4 Search results appear grouped by category. In a multidomain deployment, within the **Objects** category, the results are organized by the domains in which the objects are defined. Under the **Objects** category you can:

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.

To:	Do this:
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 a separate browser window.	Click the object name in the search results, and in the details pane click **Edit** ( ). In a multidomain deployment, if you choose to edit an object not defined within your current domain the system will prompt you to change your current domain.

Search for how to walkthroughs

Search for How To walkthroughs to access step-by-step instructions for your tasks. This feature helps you find guides for device setup and other procedures quickly.

This task is relevant when you need guidance on specific procedures or want to find walkthroughs for tasks such as device setup.

Search for How To walkthroughs about tasks you are interested in. For example, to find walkthroughs for device setup, search for the word "device." Use this task when you need clear instructions for a specific action.

Procedure

Step 1 Use one of two methods to initiate a search:

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

Step 2 Enter a search term associated with a task for which you would like to view a walkthrough. Search results appear near 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 view a walkthrough listed under **How-Tos**, click the walkthrough title in the search results list. For more information on How To walkthroughs, refer to Online help and documentation, on page 25.

After completing these steps, you will view a list of How To walkthroughs relevant to your search term, grouped by category. You can access detailed instructions for the selected task.

Switch domains on Secure Firewall Management Center

Switching domains enables users to access data and menu options specific to each domain in a multidomain deployment.

- Configure access to multiple domains for a single user account.
- Assign different privileges for each domain to the same user.

In a multidomain deployment, user role privileges determine the domains that a user can access and the privileges the user has in each domain. You can associate a single user account with multiple domains and assign different privileges for that user in each domain. For example, a user may have read-only privileges in the Global domain and 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, a tree of available domains appears. 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.

Before you begin

You do not need explicit prerequisites to switch domains. However, your user account must be associated with multiple domains and have the necessary privileges.

- Ensure your user account is assigned to more than one domain.
- Verify you have privileges in each domain you want to access.

Follow these steps to switch domains on Secure Firewall Management Center:

Procedure

From the drop-down list under your user name, choose the domain you want to access.
The domain is successfully switched.

The system displays data and menu options relevant to the selected domain, based on your assigned privileges.

What to do next

No additional steps are required after switching domains. You can repeat the process to switch to another domain as needed.

Context menus

A context menu is a web interface feature that

- provides shortcuts for accessing other features through right-click or left-click actions
- contains contents that depend on the specific page and data where you access it, and
- appears as the normal browser context menu on pages or locations that do not support it.

Context menu capabilities by location

Certain pages in the web interface support a right-click (most common) or left-click context menu that you can use as a shortcut for accessing other features. 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 context menu, the normal context menu for your browser appears.

Specific context menu capabilities by location:

- 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 an external source, using the Contextual Cross-Launch feature. For more information, see Event investigation using web-based resources.
- 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.

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.

Data sharing features with Cisco

A data sharing feature is a Cisco product capability that

- enables you to share usage metrics and analytics with Cisco
- includes features such as Cisco Success Network, web analytics, and
- may be enabled by default, and you can choose to opt out of data sharing.

Data sharing features and opt-out options

You can opt to share data with Cisco using these features:

- Cisco Success Network

Refer to Configure Cisco Success Network Enrollment

- Web analytics

  Refer to Configure web analytics

The Cisco Success Network and Cisco Support Diagnostic capabilities are enabled by default.

The Cisco Success Network capability collects customer usage metrics and statistics. Cisco analyzes product usage data and improves customer experience based on the collected metrics. To opt out of sending Cisco Success Network telemetry data to Cisco, refer to Configure Firewall Management Center to share usage metrics and statistics with Cisco. For more information about the telemetry data that Cisco collects, refer to Cisco Success Network Telemetry Data Collected from the Management Center Devices.

The Cisco Support Diagnostics capability collects essential information from your devices. Cisco uses this information to enhance your support experience. To opt out of sending Cisco Support Diagnostics metrics to Cisco, refer to Configure Firewall Management Center to share device health data with Cisco.

You can opt to share data with Cisco using web analytics. For more information, refer to Configure web analytics.

Online help and documentation

Online help, How Tos, and documentation provide support resources that

- provide context-sensitive assistance directly from the web interface
- include documentation roadmaps for additional reference information.

Access methods for online help and documentation

You can reach online help from the web interface:

- By clicking the context sensitive help link on each page.
- By choosing **Help** ( ) > **Page-level Help**.

You can find additional documentation using the documentation roadmap:

Navigating the Cisco Secure Firewall Threat Defense Documentation

How To features

How To is a widget that provides walkthroughs to help you navigate tasks on the Firewall Management Center. The walkthroughs guide you through each required step. You may need to use different UI screens 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**.

To open the How To widget, choose **Help** ( ) > **On-screen Assistance** > **How-Tos**.

For a list of walkthroughs available in your Firewall Management Center, refer to Walkthroughs in Secure Firewall Management Center.

Note Walkthroughs are generally available for all UI pages and do not depend on user role. However, if your privileges do not allow access, some menu items do not appear on the Firewall Management Center interface. As a result, you cannot run the walkthroughs on these pages.

User guides on Cisco.com

You can find documents for configuring Secure Firewall Threat Defense at Navigating the Cisco Secure Firewall Threat Defense Documentation.

License statements in the documentation

A license statement is a documentation element that

- indicates which Classic or Smart license you must assign to a managed device to enable the described feature
- shows only the highest required license for each feature because licensed capabilities are often additive, and
- uses “or” statements to specify that a particular license is required, but an additional license can add functionality.

License statement usage details

The license statement at the beginning of a section indicates which Classic or Smart license you must assign to a managed device 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, refer to Licenses.

Related Topics

Licenses

Supported devices statements in the documentation

A Supported Devices statement is a documentation element that

- appears at the beginning of a chapter or topic
- indicates that a feature is supported only on specific device series, families, or models,
- helps users identify feature support for specific devices such as Secure Firewall Threat Defense.

Platform support reference information

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

Access statements in the documentation

An access statement is a documentation element that

- indicates the predefined user roles required to perform a procedure
- allows any of the listed roles to perform the procedure, and
- provides guidance regarding access permissions for users with custom roles.

User roles and access permissions

Custom roles may have permission sets that differ from predefined roles. If you have a custom role with similar permissions, you also have access whenever a predefined role is listed for that procedure.

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 through the intrusion policy instead of the standard path through the access control policy.

IP address conventions

The system uses a set of IP address conventions to interpret IP address blocks entered using IPv4 CIDR notation or IPv6 prefix length notation, including the addresses that are not entered on the standard network boundary.

- 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 system.
- When you use CIDR or prefix length notation to specify a block of IP addresses, the 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 system uses 10.0.0.0/8.
- Cisco recommends using network IP addresses on the bit boundary when employing CIDR or prefix length notation, but the system does not enforce this requirement.

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 Firewall Management Center. Your version of the Firewall 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.