Management Center Overview

This guide applies to an *on-premises* Secure Firewall Management Center, either as your primary manager or as an analytics-only manager. When using the Cisco Defense Orchestrator (CDO) cloud-delivered management center as your primary manager, you can use an on-prem management center for analytics. Do not use this guide for CDO management; see Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator.

The Secure 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. You should use the management center if you want a multi-device manager, and you require all features on the threat defense. The management center also provides powerful analysis and monitoring of traffic and events.

Note If you have a CDO-managed device, and are using the on-prem management center for analytics only, then the on-prem management center does not support policy configuration or upgrading. Some chapters and procedures in this guide related might not apply to devices whose primary manager is CDO.

For the management center used as the primary manager: The management center is not compatible with other managers because the management center owns the threat defense configuration, and you are not allowed to configure the threat defense directly, bypassing the management center.

Quick Start: Basic Setup

The Secure Firewall feature set is powerful and flexible enough to support basic and advanced configurations. Use the following sections to quickly set up a Secure Firewall 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:

- **Management Center**
  - Cisco Secure Management Center Getting Started Guide for your hardware model, available from Cisco Secure Firewall Management Center Getting Started Guides
- **Threat Defense managed devices**
  - Cisco Firepower 1010 Getting Started Guide
  - Cisco Firepower 1100 Getting Started Guide
  - Cisco Firepower 2100 Getting Started Guide
  - Cisco Secure Firewall 3100 Getting Started Guide
  - Cisco Firepower 4100 Getting Started Guide
  - Cisco Secure Firewall 4200 Getting Started Guide
  - Cisco Firepower 9300 Getting Started Guide
  - Cisco Secure Firewall Threat Defense for the ISA 3000 Using Secure Firewall Management Center 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: Navigating the Cisco Secure Firewall Threat Defense Documentation.

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 Secure Firewall Compatibility Guide*.

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

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

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

Logging In for the First Time

Before logging in to a new management center 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 that you log in to a new management center (or a management center newly restored to factory defaults), use the **admin** account for either the CLI or the web interface and follow the instructions in the *Cisco Secure Firewall Management Center Getting Started Guide* for your management center model. When 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 for Management Center. 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 or Edit an Internal User.)
- The following network settings the management center 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 management center web interface; see Modify Management Center Management Interfaces and Time Synchronization for more information.

- As part of the initial configuration, the system schedules weekly GeoDB updates. We recommend you review this task and make changes if necessary, as described in Schedule GeoDB Updates.
- As part of the initial configuration, the system schedules weekly downloads. We recommend you review this task and make changes if necessary, as described in Automating Software Downloads.

Important This task only downloads the updates. It is your responsibility to install any updates this task downloads.

- As part of the initial configuration, the system schedules weekly configuration-only management center backups (locally stored). We recommend you review this task and make changes if necessary, as described in Schedule Management Center Backups.
- As part of the initial configuration, the system downloads and installs the latest VDB. To keep the system up to date, we recommend you schedule recurring updates as described in Vulnerability Database Update Automation.
- As part of the initial configuration, the system schedules daily intrusion rule updates. We recommend you review this task and make changes if necessary, as described in Schedule Intrusion Rule Updates.

On completion of 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 Specifying Your Home Page.)

When you complete the initial configuration, begin controlling and analyzing traffic by configuring the 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 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 in to the web interface using the **admin** account for either the web interface or CLI and perform the initial configuration as described in the *Cisco Secure Firewall Management Center Getting Started Guide* for your hardware model, available from Install and Upgrade Guides.

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 Licenses.

Step 3 Add managed devices to your deployment as described in *Add a Device to the 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 threat defense devices.
- *Interface Overview* in the Cisco Secure Firewall Management Center Device Configuration Guide, to configure interfaces on the 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.

- 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 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, see About 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:

- 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 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 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 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 management center, see Add or Edit an Internal User.
- If you want to use LDAP or RADIUS external authentication to allow access to the management center, see Configure External Authentication for the Management Center.

Step 10 Deploy configuration changes; see the Cisco Secure Firewall Management Center Device Configuration Guide.

What to do next

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

Unsupported Screens for the Latest Device Version

Although the management center can manage devices running previous versions (as specified in the compatibility matrix available at Cisco Secure Firewall Threat Defense Compatibility Guide), this guide only includes features supported on the *latest* version of device software.

For features that are only supported on old device versions, refer to the guide that matches your version.

Threat Defense Devices

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

A threat defense 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.

Threat Defense 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 Secure Firewall Threat Defense Release Notes, Cisco Secure Firewall Management Center Compatibility Guide, and Cisco Secure Firewall Threat Defense Compatibility Guide.

Features

These tables list some commonly used features.

Appliance and System Management Features

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

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	About Health Monitoring
Back up data on your appliance	Backup and restore	Backup/Restore
Upgrade to a new version	System updates	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center Cisco Secure Firewall Threat Defense Release Notes
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
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	About Licenses
Ensure continuity of appliance operations	Managed device high availability and/or management center high availability	*About Secure Firewall Threat Defense "High Availability chapter"* in the Cisco Secure Firewall Management Center Device Configuration Guide About Management Center High Availability
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

If you want to...	Configure...	As described in...
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 threat defense devices	Site-to-Site virtual private network (VPN)	*VPN Overview* in the Cisco Secure Firewall Management Center Device Configuration Guide
Establish secure tunnels between remote users and managed 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	Introduction to 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

Features for Detecting, Preventing, and Processing Potential Threats

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

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* in the Cisco Secure Firewall Management Center Device Configuration Guide
Block or monitor connections to or from IP addresses, URLs, and/or domain names	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

If you want to...	Configure...	As described in...
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
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)	*Secure Firewall 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

Integration with External Tools

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

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 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 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 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

Search the Management Center

You can use the global search feature to quickly locate and navigate to elements of your Secure Firewall 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 management center 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 14.)

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

(See Search for Objects, on page 16 .)

- How To walkthroughs.

  The search returns a list of walkthroughs that contain the search term, with links to each. (See Search for How To Walkthroughs, on page 19.)

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 management center interface to display the highlighted page. For objects and policies, this displays details about the found entity.
- Search is not case-sensitive.
- 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 management center. 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* 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

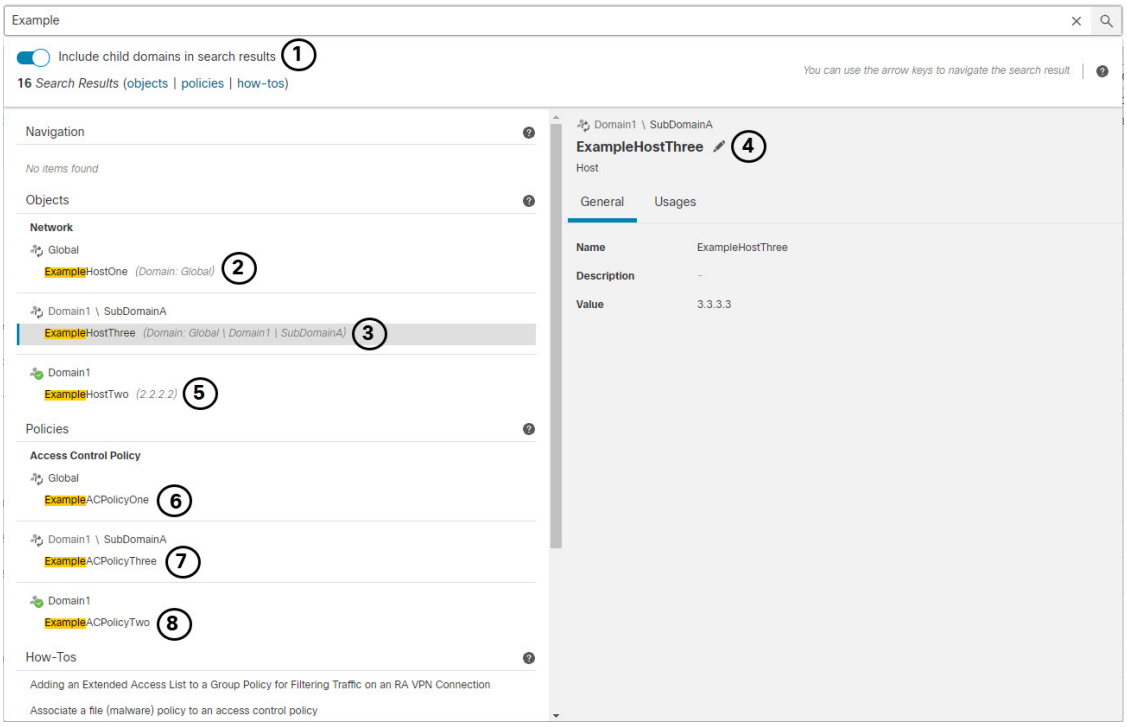
Global Search in a Multidomain Deployment

In a multidomain deployment, by default search returns only objects and policies defined within the current domain and its ancestor domains. You can see 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.

In the example screenshot below, the deployment consists of three domains at three levels: Global, Domain1, and SubDomainA. The user, whose current domain is Domain1, 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

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 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 • Intrusion Policy • Network Analysis Policy	QoS Policy FlexConfig Policy DNS Policy Malware & 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 polices 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 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, see Search the Management Center.

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

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 • 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	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

In Scope	Out of Scope
Port (objects and groups, TCP, UDP, ICMP, ICMP6, other) 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	Variable Set VPN category • Secure Client File • Custom Attribute

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 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, see Search the Management Center.

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

Step 4 Search results appear divided by category. In a multidomain deployment, within the **Objects** category the search results are grouped by the domains within which found objects are defined. Under the **Objects** 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.

To:	Do this:
View a list of polices 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

You can search for How To walkthroughs that address tasks of interest. For example, to find walkthroughs that describe device set up procedures, you can search for the term "device."

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 management center web interface, click **Search** ( ).
- With focus outside of a text box, type / (forward slash).

Step 2 Enter a search term associated with a task for which you would like to see a walkthrough. 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 view a walkthrough listed under **How-Tos**, click the walkthrough title in the search results list. For more information on How To walkthroughs, see Online Help, How To, and Documentation, on page 22.

Switching Domains on the Secure Firewall 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 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.

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.

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.

Sharing Data with Cisco

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

- Cisco Success Network

  See Configure Cisco Success Network Enrollment

- Web analytics

  See Web Analytics

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 the 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**. To open the How To widget, choose **Help** > **How-Tos**.

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 management center interface. Thereby, the walkthroughs will not execute on such pages.

The following walkthroughs are available on management center:

For a list of feature walkthroughs supported in the management center, see Feature Walkthroughs Supported in Secure Firewall Management Center.

You can find additional documentation using the documentation roadmap:

Navigating the Cisco Secure Firewall Threat Defense Documentation.

User Guides on Cisco.com

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

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

Secure Firewall Management Center

- Secure Firewall Management Center hardware appliances:

  http://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Secure Firewall 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

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

- Secure Firewall Threat Defense software:

  http://www.cisco.com/c/en/us/support/security/firepower-ngfw/tsd-products-support-series-home.html

- Secure Firewall 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

- Secure Firewall 3100:

  https://www.cisco.com/c/en/us/support/security/secure-firewall-3100-series/series.html

- Firepower 4100 series:

https://www.cisco.com/c/en/us/support/security/firepower-4100-series/tsd-products-support-series-home.html

- Secure Firewall 4200:

  https://www.cisco.com/c/en/us/support/security/secure-firewall-4200-series/series.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

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 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 Defense license.

For more information about licenses, see About Licenses.

Related Topics

About 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 Secure Firewall 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.

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 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.

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 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 management center. Your version of the 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.