

Domains

These topics describe how to manage multitenancy using domains:

- Multitenancy using domains, on page 1
- Requirements and prerequisites for domains, on page 4
- Manage domains, on page 5
- Create new domains, on page 5
- Move data between domains, on page 6
- Move devices between domains, on page 7
- History for domain management, on page 11

Multitenancy using domains

Multitenancy using domains is a segmentation approach that

- segments user access to managed devices, configurations, and events,
- allows creation of up to 100 subdomains under a top-level Global domain in two or three levels, and
- requires users to log into a single domain called the current domain.

Domain hierarchy and access control

The Firewall Management Center allows you to implement multitenancy using domains. When you log into the Firewall Management Center, you log into a single domain, called the *current domain*. Depending on your user account, you may be able to switch to other domains. You can create up to 100 subdomains under a top-level Global domain, in two or three levels.

When you log into the Firewall Management Center, you log into a single domain, referred to as the *current domain*. Depending on your user account, you may be able to switch to other domains.

In addition to any restrictions imposed by your user role, your current domain level can also limit your ability to modify various configurations. The Firewall Management Center limits most management tasks, like system software updates, to the Global domain.

The Firewall Management Center limits other tasks to *leaf domains*, which are domains with no subdomains. For example, you must associate each managed device with a leaf domain, and perform device management tasks from the context of that leaf domain. Note that each device can only belong to a single domain.

Each leaf domain builds its own network map, based on the discovery data collected by that leaf domain's devices. Events reported by a managed device (connection, intrusion, malware, and so on) are also associated with the device's leaf domain.

Domain deployment levels include:

- **One domain level: Global** - If you do not configure multitenancy, all devices, configurations, and events belong to the Global domain, which in this scenario is also a leaf domain. Except for domain management, the system hides domain-specific configurations and analysis options until you add subdomains.
- **Two domain levels: Global and second-level** - In a two-level multidomain deployment, the Global domain has direct descendant domains only. For example, a managed security service provider (MSSP) can use a single Firewall Management Center to manage network security for multiple customers.
- **Three domain levels: Global, second-level, and third-level** - In a three-level multidomain deployment, the Global domain has subdomains, at least one of which has its own subdomain.

Two-level domain deployment scenario

In a two-level multidomain deployment for an MSSP managing multiple customers:

- Administrators at the MSSP logging into the Global domain cannot view or edit customers' deployments. They must log into the respective second-level named subdomains to manage the customers' deployment.
- Administrators for each customer can log into second-level named subdomains to manage only the devices, configurations, and events applicable to their organizations. These local administrators cannot view or affect the deployments of other customers of the MSSP.

Three-level domain deployment scenario

In a three-level multidomain deployment where an MSSP customer wants to separately manage edge and internal network devices:

- Administrators for the customer logging into the second-level subdomain cannot view or edit the customer's edge network deployments. They must log into the respective leaf domain to manage the devices deployed on the network edge.
- Administrators for the customer's edge network can log into a third-level (leaf) domain to manage only the devices, configurations, and events applicable to devices deployed on the network edge. Similarly, administrators for the customer's internal network can log into a different third-level domain to manage internal devices, configurations, and events. Edge and internal administrators cannot view each other's deployment.



Note

- In a Firewall Management Center that uses multi-tenancy, SSO configuration allows the assignment of SAML users to specific subdomains. This configuration is possible only at the global domain level.
- In deployments that use multitenancy with Firewall Management Center domains, passive identity sessions apply to all managed Firewall Threat Defense devices, regardless of domain.

Related Topics

SAML Single Sign-On

Domains terminology

This documentation uses these terms when describing domains and multidomain deployments.

Domain terminology definitions:

- Global Domain: In a multidomain deployment, the top-level domain. If you do not configure multitenancy, all devices, configurations, and events belong to the Global domain. Administrators in the Global domain can manage the entire Secure Firewall System deployment.
- Subdomain: A second or third-level domain.
- Second-level domain: A child of the Global domain. Second-level domains can be leaf domains, or they can have subdomains.
- Third-level domain: A child of a second-level domain. Third-level domains are always leaf domains.
- Leaf domain: A domain with no subdomains. Each device must belong to a leaf domain.
- Descendant domain: A domain descending from the current domain in the hierarchy.
- Child domain: A domain's direct descendant.
- Ancestor domain: A domain from which the current domain descends.
- Parent domain: A domain's direct ancestor.
- Sibling domain: A domain with the same parent.
- Current domain: The domain you are logged into now. The system displays the name of the current domain before your user name at the top right of the web interface. Unless your user role is restricted, you can edit configurations in the current domain.

Domain properties

To modify a domain's properties, you must have Administrator access in that domain's parent domain.

Each domain has configurable properties that control its behavior and resource allocation:

- Name and Description: Each domain must have a unique name within its hierarchy. A description is optional.
- Parent Domain: Second- and third-level domains have a parent domain. You cannot change a domain's parent after you create the domain.
- Devices: Only leaf domains may contain devices. In other words, a domain may contain subdomains or devices, but not both. You cannot save a deployment where a non-leaf domain directly controls a device. In the domain editor, the web interface displays available and selected devices according to their current place in your domain hierarchy.
- Host Limit: The number of hosts the Firewall Management Center can monitor, and therefore store in network maps, depends on its model. In a multidomain deployment, leaf domains share the available pool of monitored hosts, but have separate network maps. To ensure that each leaf domain can populate

its network map, you can set host limits at each subdomain level. If you set a domain's host limit to `0`, the domain shares in the general pool.

Setting the host limit has a different effect at each domain level:

- Leaf — For a leaf domain, a host limit is a simple limit on the number of hosts the leaf domain can monitor.
- Second Level — For a second-level domain that manages third-level leaf domains, a host limit represents the total number of hosts that the leaf domains can monitor. The leaf domains share the pool of available hosts.
- Global — For the Global domain, the host limit is equal to the total number of hosts the Firewall Management Center can monitor. You cannot change it

The sum of subdomains' host limits can add up to more than their parent domain's host limit. For example, if the Global domain host limit is 150,000, you can configure multiple subdomains each with a host limit of 100,000. Any of those domains, but not all, can monitor 100,000 hosts.

The network discovery policy controls what happens when you detect a new host after you reach the host limit; you can drop the new host, or replace the host that has been inactive for the longest time. Because each leaf domain has its own network discovery policy, each leaf domain governs its own behavior when the system discovers a new host.

If you reduce the host limit for a domain and its network map contains more hosts than the new limit, the system deletes the hosts that have been inactive the longest.

Related Topics

Host limits

Network discovery data storage settings

Requirements and prerequisites for domains

This reference provides the requirements and prerequisites necessary for working with domains, including model support, supported domains, and required user roles.

Model support

Any.

Supported domains

Any

User roles

- Administrator

Manage domains

This task allows you to modify domain properties and structure to organize your network management hierarchy effectively.

To modify a domain's properties, you must have Administrator access in that domain's parent domain.

Before you begin

Follow these steps to manage domains:

Procedure

Step 1 Choose **System** (⚙) > **Domains**.

Step 2 Manage your domains:

- Add — Click **Add Domain**, or click **Add Subdomain** next to the parent domain; see Create new domains, on page 5.
- Edit — Click **Edit** (✎) next to the domain you want to modify; see Domain properties, on page 3.
- Delete — Click **Delete** (🗑) next to the empty domain you want to delete, then confirm your choice. Move devices from domains you want to delete by editing their destination domain.

Step 3 When you are done making changes to the domain structure and all devices are associated with leaf domains, click **Save** to implement your changes.

Step 4 If prompted, make additional changes:

- If you changed a leaf domain to a parent domain, move or delete the old network map; see Move data between domains, on page 6.
- If you moved devices between domains and must assign new policies and security zones or interface groups, see Move devices between domains, on page 7.

Your domain structure is updated according to your modifications, with devices properly organized within the domain hierarchy.

What to do next

- Configure user roles and policies (access control, network discovery, and so on) for any new domains. Update device properties as needed.
- Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Create new domains

Create new domains to organize devices into hierarchical domain structures that support policy management and device configuration.

You can create up to 100 subdomains under a top-level Global domain, in two or three levels.

You must assign all devices to a leaf domain before you can implement the domain configuration. When you add a subdomain to a leaf domain, the domain stops being a leaf domain and you must reassign its devices.

Procedure

Step 1 In a Global or a second-level domain, choose **System** (⚙) > **Domains**.

Step 2 Click **Add Domain**, or click **Add Subdomain** next to the parent domain.

Step 3 Enter a **Name** and **Description**.

Step 4 Choose a **Parent Domain**.

Step 5 On **Devices**, choose the **Available Devices** to add to the domain, then click **Add to Domain** or drag and drop into the list of **Selected Devices**.

Step 6 Optionally, click **Advanced** to limit the number of hosts the new domain may monitor; see Domain properties, on page 3.

Step 7 Click **Save** to return to the domain management page.

The system warns you if any devices are assigned to non-leaf domains. Click **Create New Domain** to create a new domain for those devices. Click **Keep Unassigned** if you plan to move the devices to existing domains.

Step 8 When you are done making changes to the domain structure and all devices are associated with leaf domains, click **Save** to implement your changes.

Step 9 If prompted, make additional changes:

- If you changed a leaf domain to a parent domain, move or delete the old network map; see Move data between domains, on page 6.
- If you moved devices between domains and must assign new policies and security zones or interface groups, see Move devices between domains, on page 7.

What to do next

- Configure user roles and policies (access control, network discovery, and so on) for any new domains. Update device properties as needed.
- Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Move data between domains

Move network maps and associated events to appropriate domains when restructuring your domain hierarchy.

Because events and network maps are associated with leaf domains, when you change a leaf domain to a parent domain, you have two choices:

- Move the network map and associated events to a new leaf domain.

- Delete the network map but retain the events. In this case, the events remain associated with the parent domain until the system prunes events as needed or as configured. Alternatively, you can delete old events manually.

Before you begin

Implement a domain configuration where a former leaf domain is now a parent domain; see Manage domains, on page 5.

Follow these steps to move data between domains:

Procedure

Step 1 For each former leaf domain that is now a parent domain:

- Choose a new **Leaf Domain** to inherit the **Parent Domain**'s events and network map.
- Choose **None** to delete the parent domain's network map, but retain old events.

Step 2 Click **Save**.

The data is moved or retained according to your selection, and the domain restructuring is complete.

What to do next

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

Move devices between domains

Move devices between domains to reorganize your network structure while preserving device configurations and ensuring proper policy assignments in the target domain.

You can move devices between domains as long as the source and the target domains are visible from the domain where you are moving the devices. Moving a device between domains can affect the configurations and policies applied to the device. The system retains the following device configurations while moving devices between domains.

- Interfaces
- Inline sets
- Routing
- DHCP
- Associated objects
- SNMP (if available)

The following changes can occur to the configuration of a device when it is moved between domains:

- If you want the system to retain the device configurations after the devices are moved to the target domain, ensure that:
  - The shared access control policies are in the Global domain. We also recommend that the other shared policies are in the Global domain.
- For VPN configurations,
  - The site-to-site VPN configurations are in the target domain.
  - The remote access VPN configurations and device certificates are in the global or target domain.
  - When you assign a remote access VPN policy to a device, you can move the device from one domain to another, only if the target domain is a descendant of the domain in which remote access VPN is configured.
- The network objects for SNMP are in the global domain.
- You can move the device into any child domain without deleting the enrolled certificate on the device. Specifically:
  - If the health policy applied to a moved device is inaccessible in the new domain, you can choose a new health policy.
  - If the access control policy assigned to a moved device is not valid or accessible in the new domain, choose a new policy. Every device must have an assigned access control policy.
  - If the interfaces on the moved device belong to a security zone that is inaccessible in the new domain, you can choose a new zone.
  - Interfaces are removed from:
    - Security zones that are inaccessible in the new domain and not used in an access control policy.
    - All interface groups.

If devices require a policy update but you do not need to move interfaces between zones, the system displays a message stating that zone configurations are up to date. For example, if a device's interfaces belong to a security zone configured in a common ancestor domain, you do not need to update zone configurations when you move devices from subdomain to subdomain.

Before you begin

- Create new domains. For more information, refer to Create new domains, on page 5.
- Implement a domain configuration where you moved a device from domain to domain and now must assign new policies and security zones; refer to Manage domains, on page 5.

Follow these steps to move devices between domains:

Procedure

Step 1 In the Global domain, choose **System** (⚙) > **Domains**.

Step 2 Edit the target domain to which you plan to move the devices.

Step 3 In the **Edit Domain** dialog box, do these actions:

a. Select the devices that you want to move and click **Add to Domain**.

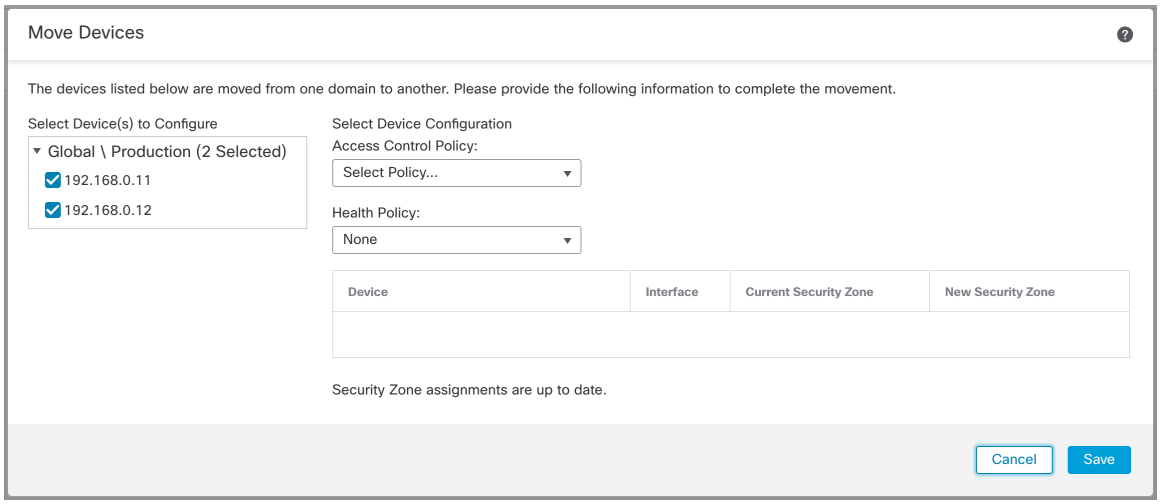
b. Click **Save**.

Step 4 On the Domains page, click **Save**.

Step 5 **(If your access control policies are not in the Global domain)** In the **Move Devices** dialog box, do these actions:

a. Under **Select Device(s) to Configure** check the device that you want to configure.

Check multiple devices to assign the same health and access control policies.



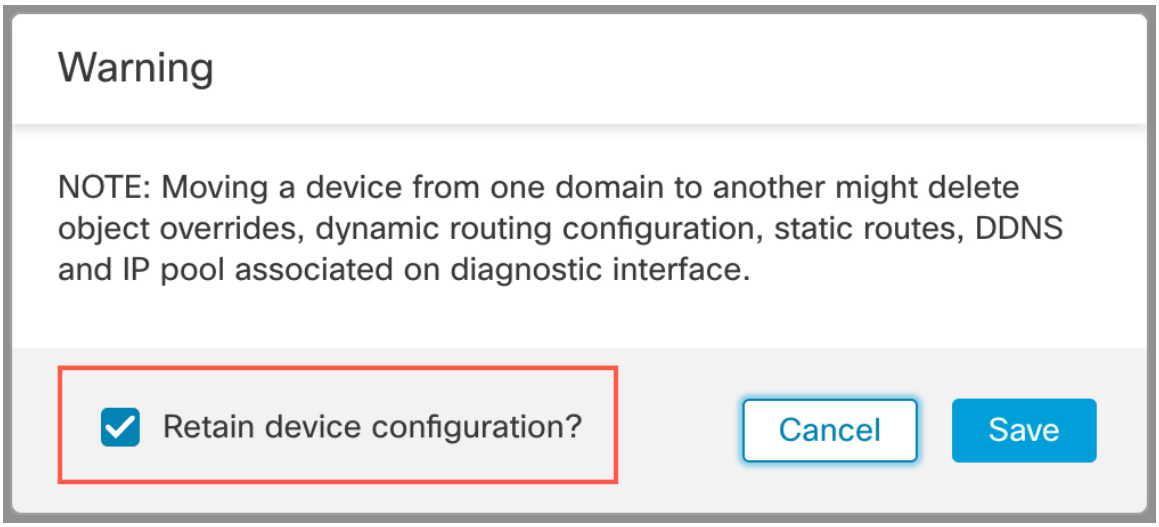
b. Choose an **Access Control Policy** to apply to the device, or choose **New Policy** to create a new policy.

c. Choose a **Health Policy** to apply to the device, or choose **None** to leave the device without a health policy.

d. If prompted to assign interfaces to new zones, choose a **New Security Zone** for each listed interface, or choose **None** to assign it later.

e. After you configure all affected devices, click **Save** to save policy and zone assignments.

Step 6 If you want to retain the device configuration after the move, check the **Retain device configuration?** check box.



If you select this option, the system retains the device configurations after the devices are moved to the target domain. If you do not select this option, you must manually update the device configurations on the moved device that were affected by the move.

This table shows how objects are handled in various scenarios.

Scenario	System Action
Objects exist in the target domain.	Reuse the objects.
Objects with the same name and value exist in the target domain.	Reuse the objects.
Objects with the same name but different values exist in the target domain.	• Network and Port—Create object overrides. • Interface Objects—Create new objects if the type is different. • Reuse all other object types depending on the name match.
Objects do not exist in the target domain.	Create new objects.

Step 7 Click **Save** to implement the domain configuration.

Step 8 After the domain configuration is complete, click **OK**.

The devices are moved to the target domain with the selected policy assignments and configuration settings.

What to do next

- Update other configurations on the moved device that were affected by the move.
- Deploy configuration changes; see the *Cisco Secure Firewall Management Center Device Configuration Guide*.

- You can manually restore the device configuration if the system fails to retain it after moving a device between domains. For more information, refer to *Export and Import the Device Configuration* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

History for domain management

This reference provides a chronological history of domain management features, including version information, platform compatibility, and detailed descriptions of feature enhancements.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Retain device configurations associated with site-to-site VPN	7.3	Any	While moving devices from one domain to another, you can now retain the device configurations associated with site-to-site VPN only if the site-to-site VPN is configured at the target domain.
Retain the device configuration	7.2	Any	You can now retain the device configuration while moving the device from one domain to another.
Increased maximum number of supported domains	6.5	Any	You can now add up to 100 domains. Previously, the maximum was 50 domains. Supported platforms: Secure Firewall Management Center