



Get Started

Security Cloud Control provides a unique view of policy management through a clear and concise interface. Below are topics that cover the basics of using Security Cloud Control for the first time.

- [Create a Security Cloud Control Tenant, on page 1](#)
- [The Security Cloud Control Dashboard, on page 3](#)
- [Create a Security Cloud Control Tenant, on page 4](#)
- [The Security Cloud Control Dashboard, on page 6](#)
- [Login Requirements for Security Cloud Control, on page 7](#)
- [Migrate to **Cisco Security Cloud Sign On** Identity Provider, on page 9](#)
- [Launch a Security Cloud Control Tenant, on page 11](#)
- [Security Cloud Control Integrations Page, on page 12](#)
- [Security Cloud Control Licenses, on page 15](#)
- [Security Cloud Control Platform Maintenance Schedule, on page 17](#)
- [Cloud-Delivered Firewall Management Center Maintenance Schedule, on page 18](#)
- [Manage Objects, on page 18](#)
- [Network Address Translation, on page 45](#)
- [Order of Processing NAT Rules, on page 45](#)
- [Network Address Translation Wizard, on page 47](#)
- [Common Use Cases for NAT, on page 48](#)

Create a Security Cloud Control Tenant

You can provision a new Security Cloud Control tenant to onboard and manage your devices. If you use an On-Premises Firewall Management Center Version 7.2 and later, and want to integrate it with the Cisco Security Cloud, you can also create a Security Cloud Control tenant as part of the integration workflow.

Procedure

1. Go to <https://us.manage.security.cisco.com/provision>.
2. Select the region where you want to provision your Security Cloud Control tenant and click **Sign Up**.
3. On the **Security Cloud Sign On** page, provide your credentials.
4. If you do not have a Security Cloud Sign On account and want to create one, click **Sign up now**.
 - a. Provide the information to create an account.

Account Sign Up

Provide following information to create enterprise account.

[Back to login page](#)

Email *

sample@cisco.com

First name *

John

Last name *

Smith

Country *

Please select *

Password *

Confirm Password *

☐ I agree to the [End User License Agreement](#) and [Privacy Statement](#).

Sign up

[Cancel](#)

Here are some tips:

- **Email:** Enter the email address that you will eventually use to log in to Security Cloud Control.
 - **Password:** Enter a strong password.
- b. Click **Sign up**. Cisco sends you a verification email to the address you registered with.
 - c. Open the email and click **Activate account** both on the mail and the **Security Cloud Sign On** page.
 - d. Configure multifactor authentication using Duo on a device of your choice and click **Log in with Duo** and **Finish**.



Note We recommend installing the Duo Security app on a mobile phone. Review [Duo Guide to Two Factor Authentication: Enrollment Guide](#) if you have questions about installing Duo.

5. Provide a name for your tenant and click **Create new account**.
6. A new Security Cloud Control tenant is created in the region that you have chosen; you will also receive an email about your Security Cloud Control tenant being created, with the details. If you are associated with multiple Security Cloud Control tenants already, on the **Choose a tenant** page, select the tenant you

just created to log in to it. If you have created a new Security Cloud Control tenant for the first time, you get logged into your tenant directly.

For information about logging on to your Security Cloud Control tenant for the first time, see [Initial Login to Your New Security Cloud Control Tenant](#).

For information about managing a Security Cloud Control tenant and various tenant settings, see [Tenant Management](#).

Upgrade your Security Cloud Control tenant to full version

If you are using a free trial version of Security Cloud Control, you will keep seeing the **You are in a free trial of** Security Cloud Control banner, with the number of days left in the trial period. You can choose to upgrade your Security Cloud Control tenant to the full version anytime during the trial period. Contact your Cisco sales representative or contact [Cisco Sales](#), and they can place an order on your behalf and get you the sales order number.

Once you obtain the sales order number, click **Upgrade to full version** on the banner and enter the order number to begin using the full version of Security Cloud Control.

Request Security Cloud Control trial period extension

If you want to continue using the trial version for 30 days, click **Request for an extension**.

The Security Cloud Control Dashboard

The Security Cloud Control dashboard is your central hub for monitoring and managing organization-level details across various categories. Upon logging in, you can access a customizable dashboard that offers critical insights and actions to optimize security and operational efficiency.

Customize Your Dashboard

Make your dashboard fit your specific needs by customizing the visible widgets.

1. On the **Home** page, click **Customize**.
2. Select or deselect the widgets you want to view on the dashboard.
3. You can drag and drop the widgets to arrange them as you prefer.

Top Information

This section provides detailed insights into various tenant-level metrics. If enabled, you can view the following widgets:

- **Configuration States:** Indicates the discrepancies between the configurations on your devices and those maintained by Security Cloud Control. This comparison helps identify any inconsistencies or conflicts that may exist.

For more information, see [Device Management](#).

- **Change Log Management:** Helps you manage the change logs for precise operational control. The widget displays **Completed** and **Pending** change logs.

For more information, see [Change Logs](#).

- **RA VPN Sessions:** Helps you monitor your Remote Access VPN sessions.

For more information, see [RA VPN Sessions](#).

- **Overall Inventory:** Helps you monitor the health and status of all devices. The widget displays the total number of devices, categorized into **Issues**, **Pending Actions**, **Other**, **Online** and devices that are nearing or have already reached their last day of hardware support.

For more information, see [All Devices](#).

- **Site-to-Site VPN:** Helps you manage and assess your site-to-site VPN connections. The widget displays the total number of VPN tunnels and the percentage that are **Active** and **Idle**.

For more information, see [Site-to-site VPN](#).

- **Accounts and Assets:**

- Helps you track and manage your multicloud accounts and resources effectively. You can launch the Multicloud Defense Controller from here.
- Click **+Add Account** to add a new account.

For more information, see [Multicloud Defense Controller](#).

- **Top Risky Destinations:** Helps you identify and monitor the top risky destinations that are granted access. The widget lists Applications and URL Categories and allows you to filter data for the last 90, 60, or 30 days. You can filter between Allowed (default) and Blocked traffic.
- **Top Intrusion and Malware Events:** Helps you monitor and respond to top intrusion and malware events. The widget displays Intrusion Events and Malware Events and allows you to filter data for the last 90, 60, and 30 days. You can filter between Allowed (default) and Blocked events.

Announcements

Click the **Announcements** icon to view the most recent Security Cloud Control features and updates. Links to related documentation are provided if you need more information on any of the items listed.

Create a Security Cloud Control Tenant

You can provision a new Security Cloud Control tenant to onboard and manage your devices. If you use an On-Premises Firewall Management Center Version 7.2 and later, and want to integrate it with the Cisco Security Cloud, you can also create a Security Cloud Control tenant as part of the integration workflow.

Procedure

1. Go to <https://us.manage.security.cisco.com/provision>.
2. Select the region where you want to provision your Security Cloud Control tenant and click **Sign Up**.
3. On the **Security Cloud Sign On** page, provide your credentials.
4. If you do not have a Security Cloud Sign On account and want to create one, click **Sign up now**.
 - a. Provide the information to create an account.

Account Sign Up

Provide following information to create enterprise account.

[Back to login page](#)

Email *

sample@cisco.com

First name *

John

Last name *

Smith

Country *

Please select *

Password *

Confirm Password *

☐ I agree to the [End User License Agreement](#) and [Privacy Statement](#).

Sign up

[Cancel](#)

Here are some tips:

- **Email:** Enter the email address that you will eventually use to log in to Security Cloud Control.
 - **Password:** Enter a strong password.
- b. Click **Sign up**. Cisco sends you a verification email to the address you registered with.
 - c. Open the email and click **Activate account** both on the mail and the **Security Cloud Sign On** page.
 - d. Configure multifactor authentication using Duo on a device of your choice and click **Log in with Duo** and **Finish**.



Note

We recommend installing the Duo Security app on a mobile phone. Review [Duo Guide to Two Factor Authentication: Enrollment Guide](#) if you have questions about installing Duo.

5. Provide a name for your tenant and click **Create new account**.
6. A new Security Cloud Control tenant is created in the region that you have chosen; you will also receive an email about your Security Cloud Control tenant being created, with the details. If you are associated with multiple Security Cloud Control tenants already, on the **Choose a tenant** page, select the tenant you

just created to log in to it. If you have created a new Security Cloud Control tenant for the first time, you get logged into your tenant directly.

For information about logging on to your Security Cloud Control tenant for the first time, see [Initial Login to Your New Security Cloud Control Tenant](#).

For information about managing a Security Cloud Control tenant and various tenant settings, see [Tenant Management](#).

Upgrade your Security Cloud Control tenant to full version

If you are using a free trial version of Security Cloud Control, you will keep seeing the **You are in a free trial of** Security Cloud Control banner, with the number of days left in the trial period. You can choose to upgrade your Security Cloud Control tenant to the full version anytime during the trial period. Contact your Cisco sales representative or contact [Cisco Sales](#), and they can place an order on your behalf and get you the sales order number.

Once you obtain the sales order number, click **Upgrade to full version** on the banner and enter the order number to begin using the full version of Security Cloud Control.

Request Security Cloud Control trial period extension

If you want to continue using the trial version for 30 days, click **Request for an extension**.

The Security Cloud Control Dashboard

The Security Cloud Control dashboard is your central hub for monitoring and managing organization-level details across various categories. Upon logging in, you can access a customizable dashboard that offers critical insights and actions to optimize security and operational efficiency.

Customize Your Dashboard

Make your dashboard fit your specific needs by customizing the visible widgets.

1. On the **Home** page, click **Customize**.
2. Select or deselect the widgets you want to view on the dashboard.
3. You can drag and drop the widgets to arrange them as you prefer.

Top Information

This section provides detailed insights into various tenant-level metrics. If enabled, you can view the following widgets:

- **Configuration States:** Indicates the discrepancies between the configurations on your devices and those maintained by Security Cloud Control. This comparison helps identify any inconsistencies or conflicts that may exist.

For more information, see [Device Management](#).

- **Change Log Management:** Helps you manage the change logs for precise operational control. The widget displays **Completed** and **Pending** change logs.

For more information, see [Change Logs](#).

- **RA VPN Sessions:** Helps you monitor your Remote Access VPN sessions.

For more information, see [RA VPN Sessions](#).

- **Overall Inventory:** Helps you monitor the health and status of all devices. The widget displays the total number of devices, categorized into **Issues**, **Pending Actions**, **Other**, **Online** and devices that are nearing or have already reached their last day of hardware support.

For more information, see [All Devices](#).

- **Site-to-Site VPN:** Helps you manage and assess your site-to-site VPN connections. The widget displays the total number of VPN tunnels and the percentage that are **Active** and **Idle**.

For more information, see [Site-to-site VPN](#).

- **Accounts and Assets:**

- Helps you track and manage your multicloud accounts and resources effectively. You can launch the Multicloud Defense Controller from here.
- Click **+Add Account** to add a new account.

For more information, see [Multicloud Defense Controller](#).

- **Top Risky Destinations:** Helps you identify and monitor the top risky destinations that are granted access. The widget lists Applications and URL Categories and allows you to filter data for the last 90, 60, or 30 days. You can filter between Allowed (default) and Blocked traffic.

- **Top Intrusion and Malware Events:** Helps you monitor and respond to top intrusion and malware events. The widget displays Intrusion Events and Malware Events and allows you to filter data for the last 90, 60, and 30 days. You can filter between Allowed (default) and Blocked events.

Announcements

Click the **Announcements** icon to view the most recent Security Cloud Control features and updates. Links to related documentation are provided if you need more information on any of the items listed.

Login Requirements for Security Cloud Control

To log in to Security Cloud Control, a customer needs an account with a SAML 2.0-compliant identity provider (IdP), a multifactor authentication provider, and [a user record in Security Cloud Control](#).

The IdP account contains the user's credentials and the IdP authenticates the user based on those credentials. Multifactor authentication provides an added layer of identity security. The Security Cloud Control user record primarily contains the username, the Security Cloud Control tenant with which they are associated, and the user's role. When a user logs in, Security Cloud Control tries to map the IdP's user ID to an existing user record on a tenant in Security Cloud Control. The user is logged in to that tenant when Security Cloud Control finds a match.

Unless your enterprise has its own single sign-on identity provider, your identity provider is Security Cloud Sign On. Security Cloud Sign On uses Duo for multifactor authentication.

Customers can [integrate their own IdP with Security Cloud Control](#) if they choose.

To log into Security Cloud Control, you must first create an account in Cisco Security Cloud Sign On, configure multifactor authentication (MFA) using Duo Security and have your tenant Super Admin create a Security Cloud Control record.

On October 14, 2019, Security Cloud Control converted all previously existing tenants to use Cisco Security Cloud Sign On as their identity provider and Duo for MFA.



Note

- If you sign in to Security Cloud Control using your own single sign-on identity provider, the transition to Cisco Security Cloud Sign On did not affect you. You continue to use your own sign-on solution.
- If you are in the middle of a free trial of Security Cloud Control, this transition did affect you.

If your Security Cloud Control tenant was created on or after October 14, 2019, see [Initial Login to Your New Security Cloud Control Tenant](#), on page 8.

If your Security Cloud Control tenant existed before October 14, 2019, see [Migrate to Cisco Security Cloud Sign On Identity Provider](#), on page 9.

Initial Login to Your New Security Cloud Control Tenant

Before You Begin



Install DUO Security. We recommend installing the Duo Security app on a mobile phone. Review [Duo Guide to Two Factor Authentication: Enrollment Guide](#) if you have questions about installing Duo.

Time Synchronization. You are going to use your mobile device to generate a one-time password. It is important that your device clock is synchronized with real time as the OTP is time-based. Make sure your device clock is set automatically or manually set it to the correct time.

Security Cloud Control uses Cisco Security Cloud Sign On as its identity provider and Duo for multifactor authentication (MFA). If you do not have a Cisco Security Cloud Sign On account, when you create a new Security Cloud Control tenant, the provisioning flow involves various steps, including creating a Security Cloud Sign On account and configuring MFA using Duo. To create a new tenant, click [here](#).

MFA provides an added layer of security in protecting your user identity. Two-factor authentication, a type of MFA, requires two components, or factors, to ensure the identity of the user logging in to Security Cloud Control. The first factor is a username and password, and the second is a one-time password (OTP), which is generated on demand.



Important

If your Security Cloud Control tenant existed before October 14, 2019, use [Migrate to Cisco Security Cloud Sign On Identity Provider](#), on page 9 for login instructions instead of this article.

What to do next?

Continue to [Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication](#). It is a four-step process. You need to complete all four steps.

Signing in to Security Cloud Control in Different Regions

These are the URLs you use to sign in to Security Cloud Control in different AWS regions:

Table 1: Security Cloud Control URLs in Different Regions

| Region | Security Cloud Control URL |
|--|---|
| Asia-Pacific and Japan (APJ) | https://apj.manage.security.cisco.com |
| Australia (AUS) | https://aus.manage.security.cisco.com |
| Europe, the Middle East, and Africa (EMEA) | https://eu.manage.security.cisco.com |
| India (IN) | https://in.manage.security.cisco.com |
| United States (US) | https://us.manage.security.cisco.com |

Troubleshooting Login Failures

Login Fails Because You are Inadvertently Logging in to the Wrong Security Cloud Control Region

Make sure you are logging in to the appropriate Security Cloud Control region. After you log in to <https://sign-on.security.cisco.com>, you will be given a choice of what region to access.

See [Signing in to Security Cloud Control in Different Regions, on page 8](#) for information about which region you should sign in to.

Migrate to Cisco Security Cloud Sign On Identity Provider

On October 14, 2019, Security Cloud Control converted all tenants to Cisco Security Cloud Sign On as their identity provider and Duo for multifactor authentication (MFA). **To log into Security Cloud Control, you must first activate your account in Cisco Secure Sign-On and configure MFA using Duo.**

Security Cloud Control requires MFA which provides an added layer of security in protecting your user identity. Two-factor authentication, a type of MFA, requires two components, or factors, to ensure the identity of the user logging into Security Cloud Control. The first factor is a username and password, and the second is a one-time password (OTP), which is generated on demand.




Note

- If you sign in to Security Cloud Control using your own single sign-on identity provider, this transition to Cisco Security Cloud Sign On and Duo does not affect you. You continue to use your own sign-on solution.
- If you are in the middle of a free trial of Security Cloud Control, this transition does apply to you.
- **If your Security Cloud Control tenant was created on or after October 14, 2019**, see [Initial Login to Your New Security Cloud Control Tenant, on page 8](#) for login instructions instead of this article.

Before You Begin

We strongly recommend the following steps prior to migrating:

-  **Install DUO Security.** We recommend installing the Duo Security app on a mobile phone. Review [Duo Guide to Two Factor Authentication: Enrollment Guide](#) if you have questions about installing Duo.
- **Time Synchronization.** You are going to use your mobile device to generate a one-time password. It is important that your device clock is synchronized with real time as the OTP is time-based. Make sure your device clock is set automatically or manually set it to the correct time.
- **Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication.** It is a four-step process. You need to complete all four steps.

Troubleshooting Login Failures after Migration

Login to Security Cloud Control Fails Because of Incorrect Username or Password

Solution If you try to log in to Security Cloud Control and you *know* you are using the correct username and password and your login is failing, or you try the "forgot password" option and cannot recover a viable password, you may have tried to log in without creating a new Cisco Security Cloud Sign On account. You need to sign up for a new Cisco Security Cloud Sign On Account.

Solution See: [Create a New Cisco Security Cloud Sign On Account and Configure Duo Multi-factor Authentication](#).

Login to the Cisco Security Cloud Sign On Dashboard Succeeds but You Can't Launch Security Cloud Control

Solution You may have created a Cisco Security Cloud Sign On account with a different username than your Security Cloud Control tenant. Contact the [Cisco Technical Assistance Center \(TAC\)](#) to standardize your user information between Security Cloud Control and Cisco Secure Sign-On.

Login Fails Using a Saved Bookmark

Solution You may be attempting to log in using an old bookmark you saved in your browser. The bookmark could be pointing to <https://cdo.onelogin.com>.

Solution Log in to <https://sign-on.security.cisco.com>.

- **Solution** If you have not yet created a Cisco Secure Sign-On account, [create an account](#).
- **Solution** If you have created your new secure sign-on account, click the Security Cloud Control tile on the dashboard that corresponds to the region in which your tenant was created:
 - **Solution** Security Cloud Control Firewall Management APJ
 - **Solution** Security Cloud Control Firewall Management Australia
 - **Solution** Security Cloud Control Firewall Management EU
 - **Solution** Security Cloud Control Firewall Management India
 - **Solution** Security Cloud Control Firewall Management US
- **Solution** Update your bookmark to point to <https://sign-on.security.cisco.com>.

Launch a Security Cloud Control Tenant

Procedure

Step 1 Click the appropriate Security Cloud Control button for your region on the Cisco Security Cloud Sign-On dashboard.

Step 2 Click the authenticator logo to choose Duo Security or Google Authenticator if you have set up both authenticators.

- If you already have a user record on an existing tenant, you are logged in to that tenant.
- If you already have a user record on several portals, you will be able to choose which portal to connect to.
- If you already have a user record on several tenants, you will be able to choose which Security Cloud Control tenant to connect to.
- If you do not already have a user record on an existing tenant, you will be able to learn more about Security Cloud Control or request a trial tenant.

The **Portals** view retrieves and displays consolidated information from multiple tenants.

See [MSSP Portal](#) for more information.

The **Tenant** view shows several tenants on which you have a user record.


The screenshot shows the Cisco Security Cloud Control interface. At the top is the Cisco logo and the text 'Security Cloud Control'. Below this is a 'Choose a tenant' section. This section is divided into two columns: 'Portals' and 'Tenants'. Each column has a search bar labeled 'Search tenant name'. Under 'Portals', there are two entries: 'US East Coast' and 'US West Coast'. Under 'Tenants', there are three entries: 'Boston Office', 'New York Office', and 'Los Angeles Office'. At the bottom center of the interface is a 'Sign Out' button.

Security Cloud Control Integrations Page

The **Integrations** page displays a list of FMCs that Security Cloud Control manages. Selecting the **FMC** tab lists the Cloud-Delivered Firewall Management Center that is linked to the Security Cloud Control account and all the on-premises management centers onboarded to Security Cloud Control. The devices that are managed by these on-prem management centers are listed in the **Security Devices** page. The **Integrations** page also lists the secure connectors under the **Secure Connectors** tab.

You can click the **FMC** tab and onboard an on-premises management center by clicking the blue plus icon



() , and perform device actions using the options in the right pane. You can also see device information such as version, number of devices being managed by the management center, device type, and the synchronization status of the device. Clicking on the managed devices icon takes you to the **Security Devices** page, where devices managed by the selected on-premises management center are filtered automatically and displayed. The **Integrations** page also allows you to select more than one on-premises management center at a time for you to perform actions on a group of management centers all at once. You cannot select any on-premises management center while the Cloud-Delivered Firewall Management Center is selected. To add a new secure connector or perform actions on existing secure connectors, choose the **Secure Connectors** tab

and click .

In the left pane, click **Administration > Firewall Management Center**.

| Name | Version | Devices | Type | Status | Last Heartbeat |
|---|------------------|---------|---------------------|------------|----------------------|
| <input checked="" type="checkbox"/> Cloud-Delivered FMC | 20240822 | 0 | Cloud-Delivered FMC | Active | 11/25/2024, 19:17:40 |
| <input type="checkbox"/> FMC-Securex-Onboarding-1675266108901 | N/A | 0 | On-Prem FMC | Read Error | - |
| <input type="checkbox"/> Responder_30.10.0.5 | 7.6.0-build 1511 | 2 | On-Prem FMC | Read Error | - |
| <input type="checkbox"/> on-prem-fmc-1.100.com_30.12.48.52 | N/A | 0 | On-Prem FMC | Read Error | - |
| <input type="checkbox"/> FMCOne_30.10.2.160 | N/A | 0 | On-Prem FMC | Read Error | - |
| <input type="checkbox"/> Responder_30.12.40.12 | N/A | 0 | On-Prem FMC | Read Error | - |
| <input type="checkbox"/> Responder_30.10.13.11 | N/A | 0 | On-Prem FMC | Read Error | - |

For your Cloud-Delivered Firewall Management Center, the Integrations page displays the following information:

- If you do not have a Cloud-Delivered Firewall Management Center deployed on your tenant, click **Enable Cloud-Delivered FMC**. See [Enable Cloud-Delivered Firewall Management Center on Your Security Cloud Control Tenant](#) for more information.
- The number of Secure Firewall Threat Defense devices deployed on the Cloud-Delivered Firewall Management Center.
- Status of the connection between Security Cloud Control and the Cloud-Delivered Firewall Management Center page.

- The last heartbeat of the Cloud-Delivered Firewall Management Center. This represents the last time the status of the Cloud-Delivered Firewall Management Center itself and the number of devices that it manages were synchronized with the table on this page.
- The hostname of the selected Cloud-Delivered Firewall Management Center.

Choose **Cloud-Delivered FMC** and using the links in the **Actions**, **Management**, or **Settings** pane, you open the Cloud-Delivered Firewall Management Center user interface to perform the configuration tasks that are associated with the link you clicked.

Actions:

- **Check For Changes:** The Device Count and Status information in the table will be updated with the information available the last time this page and the Cloud-Delivered Firewall Management Center were synchronized. Synchronization happens every 10 minutes.
- **Deployment:** Takes you to the device configuration deployment page on Cloud-Delivered Firewall Management Center. See [Deploy Configuration Changes](#).
- **Workflows:** Takes you to the **Workflows** page to monitor every process that Security Cloud Control runs when communicating with devices. See [Workflows](#) page.
- **API Explorer:** Takes you to the page that lists the Cloud-Delivered Firewall Management Center REST APIs. See [Secure Firewall Management Center REST API Guide](#).
- **Unified Events:** Takes you to the **Unified Events** page on the Cloud-delivered Firewall Management Center portal, which provides a single-screen view of various firewall events, including connection, intrusion, file, malware, and security-related connection events. For more information, see [Unified Events](#).



Note The Unified Events feature requires activation. If you have not yet activated this feature, contact your Cisco sales representative to enable it.

Management:

- **Devices:** Takes you to the Firewall Threat Defense device listing page on the Cloud-Delivered Firewall Management Center portal. See [Configure Devices](#).
- **Policies:** Takes you to the policies page on the Cloud-Delivered Firewall Management Center portal to edit system-provided access control policies and create custom access control policies. See [Manage Access Control Policies](#).
- **Objects:** Takes you to the policies page on the Cloud-Delivered Firewall Management Center portal to manage reusable objects. See [Object Management](#).
- **NAT:** Takes you to the policies page on the Cloud-Delivered Firewall Management Center portal to configure Network Address Translation policies on the Firewall Threat Defense devices. See [Manage NAT policies](#).
- **Site to Site VPN:** Takes you to the site-to-site VPN dashboard page on the Cloud-Delivered Firewall Management Center portal to configure site-to-site VPN policy between two sites. See [Site-to-Site VPNs](#).
- **Remote Access VPN:** Takes you to the remote access VPN dashboard page on the Cloud-Delivered Firewall Management Center portal to configure a remote access VPN configuration. See [Remote Access VPN](#).

- **Platform Settings:** Takes you to the platform settings page on the Cloud-Delivered Firewall Management Center portal to configure a range of unrelated features whose values you might want to share among several devices. See [Platform Settings](#).

System:

- **Configuration:** Takes you to the system configuration settings page on the Cloud-Delivered Firewall Management Center portal to configure system configuration settings. See [System Configuration](#).
- **Smart Licenses:** Takes you to the smart licenses page on the Cloud-Delivered Firewall Management Center portal to assign licenses to devices. See [Assign Licenses to Devices](#).
- **AMP Management:** Takes you to the AMP management page on the Cloud-Delivered Firewall Management Center portal that provides intelligence that the system uses to detect and block malware on your network. See [Cloud Connections for Malware Protection](#).
- **Device Health:** Takes you to the health monitoring page on the Cloud-Delivered Firewall Management Center portal that tracks various health indicators to ensure that the hardware and software in the system are working correctly. See [About Health Monitoring](#).
- **Audit:** Takes you to the audit log page on the Cloud-Delivered Firewall Management Center portal to show the generated audit record for each user interaction with the web interface.
- **Cisco Cloud Events:** Takes you to the configure Cisco Cloud events page on the Security Cloud Control portal to configure Cloud-Delivered Firewall Management Center to send events directly to SAL (SaaS). See [Send Events to SAL \(SaaS\)](#).

After opening the Cloud-Delivered Firewall Management Center page, click the blue question mark button and select **Page-level Help** to learn more about the page you are on and what further action you can take.

Support to Open Security Cloud Control and Cloud-Delivered Firewall Management Center Applications in Separate Tabs

As you configure Firewall Threat Defense devices or objects in Cloud-Delivered Firewall Management Center, you can open the appropriate configuration pages in additional browser tabs to work simultaneously in the Security Cloud Control and the Cloud-Delivered Firewall Management Center portals without logging off.

For example, you can create an object on Cloud-Delivered Firewall Management Center and simultaneously monitor event logs on Security Cloud Control that are generated from the security policies.

This feature is available for all Security Cloud Control links that navigate to the Cloud-Delivered Firewall Management Center portal. To open the Cloud-Delivered Firewall Management Center portal in a new tab:

On the Security Cloud Control portal, press and hold the Ctrl (Windows) or Command (Mac) button, then click the corresponding link.



Note A single click opens the Cloud-Delivered Firewall Management Center page in the same tab.

Here are some examples of opening the Cloud-Delivered Firewall Management Center portal page in a new tab:

- Choose **Administration > Firewall Management Center** and select **Cloud-Delivered FMC**. In the right pane, press and hold the Ctrl (Windows) or Command (Mac) button, and then click the page that you want to access.

- Choose **Objects > Other FTD Objects**.
- Click the search icon in the top-right corner of the Security Cloud Control page and enter the search strings in the search field that appears.

From the search result, press and hold the Ctrl (Windows) or Command (Mac) button, and then click the arrow icon.
- Choose **Dashboard > Quick Actions**. Press and hold the Ctrl (Windows) or Command (Mac) button, and then click **Manage FTD Policies** or **Manage FTD Objects**.



Note When you switch to a new Security Cloud Control tenant, the corresponding Cloud-Delivered Firewall Management Center portal already opened in a new tab logs out.

Related Topics

- [Managing On-Prem Firewall Management Center with Security Cloud Control Firewall Management](#)
- [Onboard an On-Prem Firewall Management Center](#)
- [Request a cloud-delivered Firewall Management Center for your Security Cloud Control tenant](#)
- [Secure Device Connector](#)
- [Secure Event Connectors](#)

Security Cloud Control Licenses

Security Cloud Control requires a base subscription for organization entitlement and device licenses for managing devices. You can buy one or more Security Cloud Control base subscriptions based on the number of tenants you require and device licenses based on the device model number and the quantity. In other words, purchasing the base subscription gives you a Security Cloud Control organization, and for every device you choose to manage using Security Cloud Control, you need separate device licenses.

To onboard and manage devices from Security Cloud Control, you need to purchase a base subscription and device-specific, term-based subscriptions based on the devices you want to manage.

Subscriptions

Security Cloud Control Firewall Management subscriptions are term-based:

- **Base** - Offers subscriptions for one, three, and five years, and provides entitlement to access the Security Cloud Control organization and onboard adequately licensed devices.
- **Device License** - Offers subscriptions for one, three, and five years for any supported device you choose to manage. For example, you can choose to manage a Cisco Firepower 1010 device using Security Cloud Control for three years, if you purchase a three-year software subscription to the Cisco Firepower 1010 device.

See [Software and Hardware Supported by Security Cloud Control](#) for more information on Cisco security devices that Security Cloud Control supports.



Note Catalyst SD-WAN doesn't require an additional license. Customers using DNA or WAN Essentials license will be able to integrate with Security Cloud Control.



Important You do not require two separate device licenses to manage a high availability device pair in Security Cloud Control. If you have a high availability pair, purchasing one device license is sufficient, as Security Cloud Control considers the pair of high availability devices as one single device.



Note You cannot manage Security Cloud Control licensing through the Cisco smart licensing portal.

Software Subscription Support

The Security Cloud Control base subscription includes software subscription support that is valid for the term of the subscription and provides access to software updates, major upgrades, and Cisco Technical Assistance Center (TAC), at no extra cost. While the software support is selected by default, you can also leverage the Security Cloud Control solution support based on your requirement.

Cloud-Delivered Firewall Management Center and Threat Defense Licenses

You do not have to purchase a separate license to use the Cloud-Delivered Firewall Management Center in Security Cloud Control; the base subscription for a Security Cloud Control tenant includes the cost for the Cloud-Delivered Firewall Management Center.

Cloud-delivered Firewall Management Center Evaluation License

The cloud-delivered Firewall Management Center comes provisioned with a 90-day evaluation license. After the evaluation period has elapsed, you can still onboard Firewall Threat Defense devices to the cloud-delivered Firewall Management Center. However, any manually triggered or scheduled deployments are blocked, until you register your cloud-delivered Firewall Management Center with the Cisco Smart Software Manager (CSSM). As your evaluation license approaches the expiry date, Security Cloud Control notifies you through alerts on the notifications window.

We also recommend that, after registering to CSSM, you purchase the required licenses for the features you want to use. Purchasing licenses keeps the cloud-delivered Firewall Management Center from going out of compliance.

To know more about how to register the cloud-delivered Firewall Management Center with CSSM, see [Register the Management Center with the Smart Software Manager](#).

To learn how to get a cloud-delivered Firewall Management Center provisioned on your Security Cloud Control tenant, see [Request a Cloud-delivered Firewall Management Center for your Security Cloud Control Tenant](#).



Note The Cloud-Delivered Firewall Management Center does not support specific license reservation (SLR) for devices in air-gapped networks.

Threat Defense Licenses for Cloud-Delivered Firewall Management Center

You need individual licenses for each Secure Firewall Threat Defense device managed by the Cloud-Delivered Firewall Management Center. See [Licensing](#) in *Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control Firewall Management* for information.

To know how Security Cloud Control handles licensing for the devices migrated to the Cloud-Delivered Firewall Management Center, see [Migrate Threat Defense from Management Center to Cloud](#).



Note The Talos certificate for Evaluation Mode in Secure Firewall version 7.6.0 is set to expire on March 31, 2025. After this date, access to Talos-hosted services in Evaluation Mode (specifically those related to web reputation / categorization lookups) will be discontinued.

Security Cloud Control Platform Maintenance Schedule

Security Cloud Control updates its platform every week with new features and quality improvements. Updates are made during a 3-hour period according to this schedule:

| Day of the Week | Time of Day (24-hour time, UTC) |
|-----------------|------------------------------------|
| Thursday | 09:00 UTC - 12:00 UTC |

During this maintenance period, you can still access your organization and if you have a cloud-delivered Firewall Management Center or Multicloud Defense Controller, you can access those portals as well. Additionally, the devices that you have onboarded to Security Cloud Control continue to enforce their security policies.



- Note**
- We advise against using Security Cloud Control to deploy configuration changes on the devices it manages during maintenance periods.
 - If there is any issue that stops Security Cloud Control from communicating, we address that failure on all affected tenants as quickly as possible, even if it is outside the maintenance window.

Cloud-Delivered Firewall Management Center Maintenance Schedule

Customers who have a cloud-delivered Firewall Management Center deployed on their tenant are notified approximately 1 week before Security Cloud Control updates the cloud-delivered Firewall Management Center environment. Super Admin and Admin users of the tenant are notified by email. Security Cloud Control also displays a banner on its home page notifying all users of upcoming updates.




Note

- We advise you not to use Cloud-Delivered Firewall Management Center to deploy configuration changes on the devices it manages during maintenance periods.
- If there is any issue that stops Security Cloud Control or cloud-delivered Firewall Management Center from communicating, that failure is addressed on all affected tenants as quickly as possible, even if it is outside the maintenance window.




Manage Objects

An object is a container of information that you can use in one or more security policies. Objects make it easy to maintain policy consistency. You can create a single object, use it different policies, modify the object, and that change is propagated to every policy that uses the object. Without objects, you would need to modify all the policies, individually, that require the same change.

When you onboard a device, Security Cloud Control recognizes all the objects used by that device, saves them, and lists them on the **Objects** page. From the **Objects** page, you can edit existing objects and create new ones to use in your security policies.

Security Cloud Control calls an object used on multiple devices a **shared object** and identifies them in the **Objects** page with this badge .

Sometimes a shared object develops some "issue" and is no longer perfectly shared across multiple policies or devices:

- **Duplicate objects** are two or more objects on the same device with different names but the same values. These objects usually serve similar purposes and are used by different policies. Duplicate objects are identified by this issue icon: .
- **Inconsistent objects** are objects on two or more devices with the same name but different values. Sometimes users create objects in different configurations with same name and content but over time the values of these objects diverge which creates the inconsistency. Inconsistent objects are identified by this issue icon: .
- **Unused objects** are objects that exist in a device configuration but are not referenced by another object, an access-list, or a NAT rule. Unused objects are identified by this issue icon: .

You can also create objects for immediate use in rules or policies. You can create an object that is unassociated with any rule or policy. When you use that unassociated object in a rule or policy, Security Cloud Control creates a copy of it and uses the copy.

You can view the objects managed by Security Cloud Control by navigating to the **Objects** menu or by viewing them in the details of a network policy.

Security Cloud Control allows you to manage network and service objects across supported devices from one location. With Security Cloud Control, you can manage objects in these ways:

- Search for and [filter all your objects](#) based on a variety of criteria.
- Find duplicate, unused, and inconsistent objects on your devices and consolidate, delete, or resolve those object issues.
- Find unassociated objects and delete them if they are unused.
- Discover shared objects that are common across devices.
- Evaluate the impact of changes to an object on a set of policies and devices before committing the change.
- Compare a set of objects and their relationships with different policies and devices.
- Capture objects in use by a device after it has been on-boarded to Security Cloud Control.

If you have issues with creating, editing, or reading objects from an onboarded device, see [Troubleshoot Security Cloud Control](#) for more information.

Object Types

The following table describes the objects that you can create for your devices and manage using Security Cloud Control.

Table 2: On-Premises Secure Firewall Management Center Object Types

| Object | Description |
|-------------------------|--|
| Network | Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks. |
| Service | Service objects, service groups, and port groups are reusable components that contain protocols or ports considered part of the TCP/IP protocol suite. |

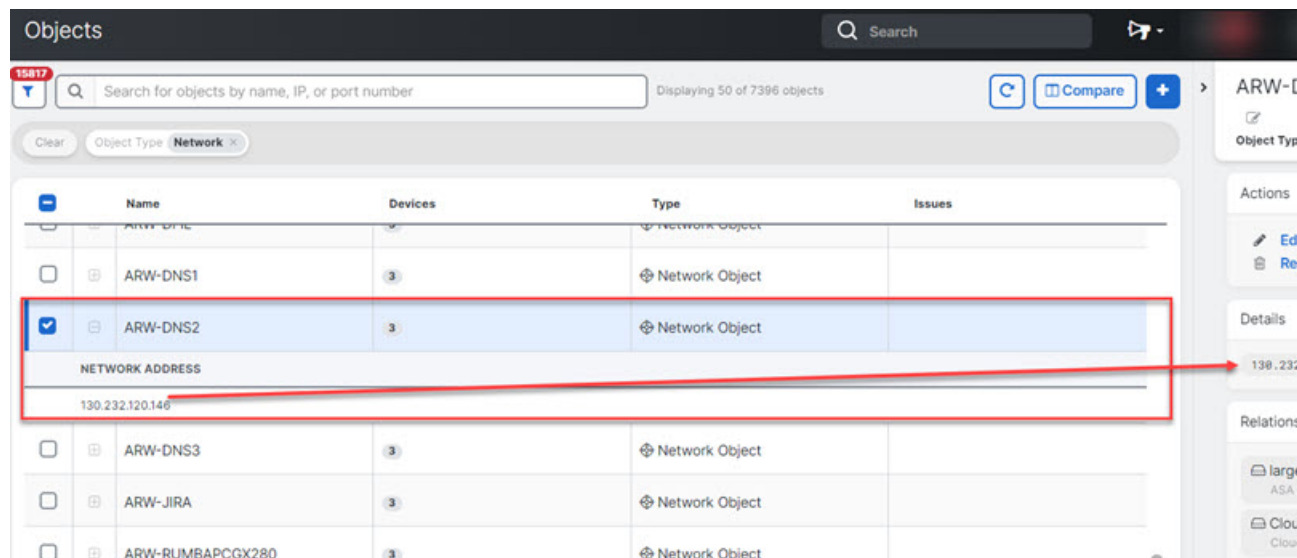
Shared Objects

Security Cloud Control calls objects on multiple devices with the same name and same contents, **shared objects**. Shared objects are identified by this icon



on the **Objects** page. Shared objects make it easy to maintain policies because you can modify an object in one place and that change affects all the other policies that use that object. Without shared objects, you would need to modify all the policies individually that require the same change.

When looking at a shared object, Security Cloud Control shows you the contents of the object in the object table. Shared objects have exactly the same contents. Security Cloud Control shows you a combined or "flattened" view of the elements of the object in the details pane. Notice that in the details pane, the network elements are flattened into a simple list and not directly associated with a named object.



Object Overrides

An object override allows you to override the value of a shared network object on specific devices. Security Cloud Control uses the corresponding value for the devices that you specify when configuring the override. Although the objects are on two or more devices with the same name but different values, Security Cloud Control doesn't identify them as **Inconsistent objects** only because these values are added as overrides.

You can create an object whose definition works for most devices, and then use overrides to specify modifications to the object for the few devices that need different definitions. You can also create an object that needs to be overridden for all devices, but its use allows you to create a single policy for all devices. Object overrides allow you to create a smaller set of shared policies for use across devices without giving up the ability to alter policies when needed for individual devices.

For example, consider a scenario where you have a printer server in each of your offices, and you have created a printer server object `print-server`. You have a rule in your ACL to deny printer servers from accessing the internet. The printer server object has a default value that you want to change from one office to another. You can do this by using object overrides and maintain rule and "printer-server" object consistent across all locations, although their values may be different.

Editing Shared Network Object

Object Name *

print-server

Devices

2 Devices

Usage

0 Rule Sets

Description

printer server object

Default Value

eq

126.0.1.0

ASAv-99-18

Override Values

Enter a value to add it

| Value | Devices | |
|-----------|--------------------------|--|
| 126.0.2.4 | Pasadena-ftd-730-516-... | |
| 126.0.1.6 | BGL_FTD_7.3 | |
| 126.0.1.9 | connected_fmc | |

Cancel

Save


**Note**

If there are inconsistent objects, you can combine them into a single shared object with overrides. For more information, see [Resolve Inconsistent Object Issues](#).

Unassociated Objects

You can create objects for immediate use in rules or policies. You can also create an object that is unassociated with any rule or policy. When you use that unassociated object in a rule or policy, Security Cloud Control creates a copy of it and uses the copy. The original unassociated object remains among the list of available objects until it is either deleted by a nightly maintenance job, or you delete it.

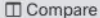
Unassociated objects remain in Security Cloud Control as a copy to ensure that not all configurations are lost if the rule or policy associated with the object is deleted accidentally.

In the left pane, click **Objects** >  and check the **Unassociated** checkbox.

Compare Objects


Procedure

- Step 1** In the left pane, click **Objects** and choose an option.
- Step 2** Filter the objects on the page to find the objects you want to compare.

- Step 3** Click the **Compare** button 
- Step 4** Select up to three objects to compare.
- Step 5** View the objects, side-by-side, at the bottom of the screen.
- Click the up and down arrows in the Object Details title bar to see more or less of the Object Details.
 - Expand or collapse the Details and Relationships boxes to see more or less information.
- Step 6** (Optional) The Relationships box shows how an object is used. It may be associated with a device or a policy. If the object is associated with a device, you can click the device name and then click **View Configuration** to see the configuration of the device. Security Cloud Control shows you the device's configuration file and highlights the entry for that object.
-

Filters

You can use many different filters on the **Security Devices** and **Objects** pages to find the devices and objects you are looking for.

To filter, click  in the left-hand pane of the Security Devices, Policies, and Objects tabs:

The Security Devices filter allows you to filter by device type, hardware and software versions, snort version, configuration status, connection states, conflict detection, and secure device connectors, and labels. You can apply filters to find devices within a selected device type tab. You can use filters to find devices within the selected device type tab.

The object filter allows you to filter by device, issue type, shared objects, unassociated objects, and object type. You can include system objects in your results or not. You can also use the search field to search for objects in the filter results that contain a certain name, IP address, or port number.

The object type filter allows you to filter objects by type, such as network object, network group, URL object, URL group, service object, and service group. The shared objects filter allows filtering objects having default values or override values.

When filtering devices and objects, you can combine your search terms to create several potential search strategies to find relevant results.

In the following example, filters are applied to search for objects that are "Issues (Unused OR Inconsistent) AND Shared Objects (with Default Values OR Additional Values) AND Unassociated Objects."

Filter

Filter by Device

Show System-Defined Objects

Issues 18661

Unused 4754

Duplicate 13846

Inconsistent 61

Ignored Issues

Ignored

Shared Objects

Default Values

Override Values

Additional Values

Unassociated Objects

Unassociated


Object Type

Network

Protocol

Service

Object Filters

To filter, click  in the left-hand pane of the Objects tab:

- **Filter by Device:** Lets you pick a specific device so that you can see objects found on the selected device.
- **Issues:** Lets you pick unused, duplicate, and inconsistent objects to view.
- **Ignored Issues:** Lets you view all the objects whose inconsistencies you had ignored.
- **Shared Objects:** Lets you view all the objects that Security Cloud Control has found to be shared on more than one device. You can choose to see shared objects with only default values or override values, or both.
- **Unassociated Objects:** Lets you view all the objects that are not associated with any rule or policy.
- **Object Type:** Lets you select an object type to see only those type of objects that you have selected, such as network objects, network groups, URL objects, URL groups, service objects, and service groups.

Sub filters – Within each main filter, there are sub-filters you can apply to further narrow down your selection. These sub-filters are based on Object Type – Network, Service, Protocol, etc.

The selected filters in this filter bar would return objects that match the following criteria:

- * Objects that are on one of two devices. (Click **Filter by Device** to specify the devices.) AND are
- * **Inconsistent** objects AND are
- * **Network** objects OR **Service** objects AND
- * Have the word "**group**" in their object naming convention

Because **Show System Objects** is checked, the result would include both system objects and user-defined objects.

Show System-Defined Objects Filter

Some devices come with predefined objects for common services. These system objects are convenient because they are already made for you and you can use them in your rules and policies. There can be many system objects in the objects table. System objects cannot be edited or deleted.


Show System-Defined Objects is **off** by default. To display system objects in the object table, check **Show System-Defined Objects** in the filter bar. To hide system objects in the object table, leave Show System Objects unchecked in the filter bar.

If you hide system objects, they will not be included in your search and filtering results. If you show system objects, they will be included in your object search and filtering results.

Configure Object Filters

You can filter on as few or as many criteria as you want. The more categories you filter by, the fewer results you should expect.

Procedure

-
- Step 1** In the left pane, click **Objects**.
- Step 2** Open the filter panel by clicking the filter icon  at the top of the page. Uncheck any filters that have been checked to make sure no objects are inadvertently filtered out. Additionally, look at the search field and delete any text that may have been entered in the search field.
- Step 3** If you want to restrict your results to those found on particular devices:
- a. Click **Filter By Device**.
 - b. Search all the devices or click a device tab to search for only devices of a certain kind.
 - c. Check the device you want to include in your filter criteria.
 - d. Click **OK**.
- Step 4** Check **Show System Objects** to include system objects in your search results. Uncheck **Show System Objects** to exclude system objects from your search results.
- Step 5** Check the object **Issues** you want to filter by. If you check more than one issue, objects in any of the categories you check are included in your filter results.

- Step 6** Check **Ignored** issues if you want to see the object that had issues but was ignored by the administrator.
- Step 7** Check the required filter in **Shared Objects** if you are filtering for objects shared between two or more devices.
- **Default Values:** Filters objects having only the default values.
 - **Override Values:** Filters objects having overridden values.
 - **Additional Values:** Filters objects having additional values.
- Step 8** Check **Unassociated** if you are filtering for objects that are not part of any rule or policy.
- Step 9** Check the **Object Types** you want to filter by.
- Step 10** You can also add an object name, IP address, or port number to the Objects search field to find objects with your search criteria among the filtered results.

When to Exclude a Device from Filter Criteria

When adding a device to filtering criteria, the results show you the objects on a device but not the relationships of those objects to other devices. For example, assume **ObjectA** is shared between ASA1 and ASA2. If you were to filter objects to find shared objects on ASA1, you would find **ObjectA** but the **Relationships** pane would only show you that the object is on ASA1.

To see all the devices to which an object is related, don't specify a device in your search criteria. Filter by the other criteria and add search criteria if you choose to. Select an object that Security Cloud Control identifies and then look in the Relationships pane. You will see all the devices and policies the object is related to.

Unignore Objects

One way to resolve unused, duplicate, or inconsistent objects is to ignore them. You may decide that though an object is **unused**, a **duplicate**, or **inconsistent**, there are valid reasons for that state and you choose to leave the object issue unresolved. At some point in the future, you may want to resolve those ignored objects. As Security Cloud Control does not display ignored objects when you search for object issues, you will need to filter the object list for ignored objects and then act on the results.

Procedure

- Step 1** In the left pane, click **Objects** and choose an option.
- Step 2** [Filter and search for ignored objects.](#)
- Step 3** In the **Object** table, select the object you want to unignore. You can unignore one object at a time.
- Step 4** Click **Unignore** in the details pane.
- Step 5** Confirm your request. Now, when you filter your objects by issue, you should find the object that was previously ignored.

Deleting Objects

You can delete a single object or multiple objects.

Delete a Single Object




Caution

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.


Procedure

- Step 1** In the left pane, click **Objects**.
- Step 2** Locate the object you want to delete by using object filters and the search field, and select it.
- Step 3** Review the **Relationships** pane. If the object is used in a policy or in an object group, you cannot delete the object until you remove it from that policy or group.
- Step 4** In the Actions pane, click the **Remove** icon .
- Step 5** Confirm that you want to delete the object by clicking **OK**.
- Step 6** [Review and deploy](#) the changes you made, or wait and deploy multiple changes at once.

Delete a Group of Unused Objects

As you onboard devices and start resolving object issues, you find many unused objects. You can delete up to 50 unused objects at a time.

Procedure

- Step 1** Use the **Issues** filter to find **unused** objects. You can also use the Device filter to find objects that are not associated with a device by selecting **No Device**. Once you have filtered the object list, the object checkboxes appear.
- Step 2** Check the **Select all** checkbox in the object table header to select all the objects found by the filter that appear in the object table; or, check individual checkboxes for individual objects you want to delete.
- Step 3** In the Actions pane, click the **Remove** icon .
- Step 4** [Review and deploy](#) now the changes you made, or wait and deploy multiple changes at once.

Network Objects

A **network object** can contain a host name, a network IP address, a range of IP addresses, a fully qualified domain name (FQDN), or a subnetwork expressed in CIDR notation. **Network groups** are collections of

network objects and other individual addresses or subnetworks that you add to the group. Network objects and network groups are used in access rules, network policies, and NAT rules.

Note that not all platforms support network objects, such as Cisco Meraki and Multicloud Defense; when you share dynamic objects, Security Cloud Control automatically translates the appropriate information from the originating platform or device into a set of usable information that Security Cloud Control can use.

Reusing Network Objects Across Products

If you have a Security Cloud Control tenant with a Cloud-Delivered Firewall Management Center and one or more on-premises management centers onboarded to your tenant:

- When you create a Secure Firewall Threat Defense, FDM-managed Firewall Threat Defense, ASA, or Meraki network object or group, a copy of the object is also added to the objects list on the **Objects** page used when configuring Cloud-Delivered Firewall Management Center, and vice versa.
- When you create a Secure Firewall Threat Defense, FDM-managed Firewall Threat Defense, or ASA network object or group, an entry is created in the **Devices with Pending Changes** page for each On-Premises Firewall Management Center for which **Discover & Manage Network Objects** is enabled. From this list, you can choose and deploy the object to the on-premises management center on which you want to use the object and discard the ones that you do not want. Navigate , **Administration** > **Firewall Management Center** select the on-premises management center, and click **Objects** to see your objects in the On-Premises Firewall Management Center user interface and assign them to policies.

Changes you make to network objects or groups on either page apply to the object or group instance on both pages. Deleting an object from one page also deletes the corresponding copy of the object from the other page.

Exceptions:

- If a network object of the same name already exists for Cloud-Delivered Firewall Management Center, the new Secure Firewall Threat Defense, FDM-managed Firewall Threat Defense, ASA, or Meraki network object will not be replicated on the **Objects** page of Security Cloud Control.
- Network objects and groups in onboarded Firewall Threat Defense devices that are managed by on-premises Secure Firewall Management Center are not replicated and cannot be used in Cloud-Delivered Firewall Management Center.

Note that for on-premises Secure Firewall Management Center instances that have been *migrated* to Cloud-Delivered Firewall Management Center, network objects and groups *are* replicated to the Security Cloud Control objects page if they are used in policies that were deployed to FTD devices.

- Sharing Network Objects between Security Cloud Control and Cloud-Delivered Firewall Management Center is automatically enabled on new tenants but must be requested for existing tenants. If your network objects are not being shared with Cloud-Delivered Firewall Management Center, [contact TAC](#) to have the features enabled on your tenant.
- Sharing network objects between Security Cloud Control and On-Premises Management Center is not automatically enabled on Security Cloud Control for new on-premises management centers onboarded to Security Cloud Control. If your network objects are not being shared with On-Premises Management Center, ensure the **Discover & Manage Network Objects** toggle button is enabled for the on-premises management center in **Settings** or [contact TAC](#) to have the features enabled on your tenant.

Viewing Network Objects

Network objects you create using Security Cloud Control and those Security Cloud Control recognizes in an onboarded device's configuration are displayed on the Objects page. They are labeled with their object type. This allows you to filter by object type to quickly find the object you are looking for.

When you select a network object on the Objects page, you see the object's values in the Details pane. The Relationships pane shows you if the object is used in a policy and on what device the object is stored.

When you click on a network group, you see the contents of that group. The network group is a conglomerate of all the values given to it by the network objects.

Create or Edit ASA Network Objects and Network Groups

An **ASA network object** can contain a hostname, an IP address, or a subnet address expressed in CIDR notation. **Network groups** are conglomerates of network objects, network groups, and IP addresses that are used in access rules, network policies, and NAT rules. You can create, read, update, and delete network objects and network groups using Security Cloud Control.

Table 3: Permitted Values of ASA Network Objects and Groups

| Device type | IPv4 / IPv6 | Single Address | Range of addresses | Partially Qualified Domain Name (PQDN) | Subnet using CIDR Notation |
|-------------|-------------|----------------|--------------------|--|----------------------------|
| ASA | IPv4 / IPv6 | Yes | Yes | Yes | Yes |



Note If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.



Caution If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Create an ASA Network Object

A **network object** can contain a host name, a network IP address, a range of IP addresses, a fully qualified domain name (FQDN), or a subnetwork expressed in CIDR notation. Network objects are used in access rules,

network policies, and NAT rules. You can create, update, and delete network objects and network groups using Security Cloud Control.




Note If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.

Procedure

Step 1 In the left pane, click **Manage > Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **ASA > Network**.

Step 4 Enter an object name.

Step 5 Select **Create a network object**.

Step 6 (optional) Enter an object description.

Step 7 In the **Value** section, add the IP address information in one of these ways:

- Select **eq** and then enter a single IP address, a subnet address using CIDR notation, or a Partially Qualified Domain Name (PQDN).
- Select **range** and then enter a range of IP addresses. Enter the range with the beginning and ending address in the range separated by a space. For example, 10.1.1.1 10.1.1.255 or 2001:DB8:1::1 2001:DB8:1::3

Step 8 Click **Add**.

Important

The newly created network objects aren't associated with any ASA device as they aren't part of any rule or policy. To see these objects, select the **Unassociated** objects category in object filters.

For more information, see [Object Filters](#). Once you use the unassociated objects in a device's rule or policy, such objects are associated with that device.

Create an ASA Network Group


A **network group** can contain IP address values, network objects, and network groups. When you are creating a new network group, you can search for existing objects by their name, IP addresses, IP address range, or FQDN and add them to the network group. If the object isn't present, you can instantly create that object in the same interface and add it to the network group. Network groups can contain both IPv4 and IPv6 addresses.



Note If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.

Procedure

-
- Step 1** In the left pane, click **Manage > Objects**.
- Step 2** Click the blue plus button  to create an object.
- Step 3** Click **ASA > Network**.
- Step 4** Enter an **Object Name**.
- Step 5** Select **Create a network group**.
- Step 6** (optional) Enter an object description.
- Step 7** In the **Values** field, enter a value or object name. When you start typing, Security Cloud Control provides object names or values that match your entry.
- Step 8** You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.
- Step 9** If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.
- Step 10** If you have entered a value or object that is not present, you can perform one of the following:
- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the check mark to save it.
 - Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the check mark to save it.
 - Click **Add Value** to create an inline value without using an object. Enter a value and click the check mark to save it.
- It is possible to create a new object even though the value is already present. You can make changes to those objects and save them.
- Note**
You can click the edit icon to modify the details. Clicking the delete button doesn't delete the object itself; instead, it removes it from the network group.
- Step 11** After adding the required objects, click **Add** to create a new network group.
- Step 12** [Preview and Deploy Configuration Changes for All Devices](#).
-

Edit an ASA Network Object


**Caution**

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

- Step 1** In the left pane, click **Manage > Objects**.
 - Step 2** Locate the object you want to edit by using object filters and search field.
 - Step 3** Select the network object and click the edit icon  in the **Actions** pane.
 - Step 4** Edit the values in the dialog box in the same fashion that you created in the procedures above.
- Note**
Click the delete icon next to remove the object from the network group.
- Step 5** Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
 - Step 6** Click **Confirm** to finalize the change to the object and any devices affected by it.

Edit an ASA Network Group

**Caution**


If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.


Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

- Step 1** In the left pane, click **Manage > Objects**.
- Step 2** Locate the network group you want to edit by using object filters and search field.

Step 3 Select the network group and click the edit icon  in the **Actions** pane.

Step 4 If you want to change the objects or network groups that are already added to the network group, perform the following steps:

- a. Click the edit icon  appearing beside the object name or network group to modify them.
- b. Click the checkmark to save your changes.

Note

You can click the remove icon to delete the value from a network group.

Step 5 If you want to add new network objects or network groups to this network group, you have to perform the following steps:

- a. In the **Values** field, enter a new value or the name of an existing network object. When you start typing, Security Cloud Control provides object names or values that match your entry. You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.
- b. If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object, or network group to the new network group.
- c. If you have entered a value or object that is not present, you can perform one of the following:
 - Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
 - Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.
 - Click **Add Value** to create an inline value without using an object. Enter a value and click the checkmark to save it.

It is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Step 6 Click **Save**. Security Cloud Control displays the policies that will be affected by the change.

Step 7 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 8 [Preview and Deploy Configuration Changes for All Devices](#).

Add Additional Values to a Shared Network Group in Security Cloud Control

The values in a shared network group that are present on all devices associated with it are called "default values." Security Cloud Control allows you to add "additional values" to the shared network group and assign those values to some devices associated with that shared network group. When Security Cloud Control deploys the changes to the devices, it determines the contents and pushes the "default values" to all devices associated with the shared network group and the "additional values" only to the specified devices.

For example, consider a scenario where you have four AD main servers in your head office that should be accessible from all your sites. Therefore, you have created an object group named "Active-Directory" to use it in all your sites. Now you want to add two more AD servers to one of your branch offices. You can do this by adding their details as additional values specific to that branch office on the object group "Active-Directory."

These two servers do not participate in determining whether the object "Active-Directory" is consistent or shared. Therefore, the four AD main servers are accessible from all your sites, but the branch office (with two additional servers) can access two AD servers and four AD main servers.

**Note**

If there are inconsistent shared network groups, you can combine them into a single shared network group with additional values. See [Resolve Inconsistent Object Issues](#) for more information.

**Caution**

If Cloud-Delivered Firewall Management Center is deployed on your tenant:


Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Manage > Objects**.

Step 2 Locate the shared network group that you want to edit by using object filters and search field.

Step 3 Click the edit icon  in the **Actions** pane.

- The **Devices** field shows the devices that the shared network group is present.
- The **Usage** field shows the rulesets associated with the shared network group.
- The **Default Values** field specifies the default network objects and their values associated with the shared network group that was provided during their creation. Next to this field, you can see the number of devices that contain this default value, and you can click to see their names and device types. You can also see the rulesets associated with this value.

Step 4 In the **Additional Values** field, enter a value or name. When you start typing, Security Cloud Control provides object names or values that match your entry.

Step 5 You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.

Step 6 If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.

Step 7 If you have entered a value or object that is not present, you can perform one of the following:

- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
- Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

- Click **Add Value** to create an inline value without using an object. Enter a value and click the checkmark to save it.

It is possible to create a new object even though the value is already present. You can make changes to those objects and save them.

- Step 8** In the **Devices** column, click the cell associated with the newly added object and click **Add Devices**.
- Step 9** Select the devices that you want and click **OK**.
- Step 10** Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
- Step 11** Click **Confirm** to finalize the change to the object and any devices affected by it.
- Step 12** [Preview and Deploy Configuration Changes for All Devices](#).

Edit Additional Values in a Shared Network Group in Security Cloud Control






Caution

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

- Step 1** In the left pane, click **Manage > Objects**.
- Step 2** Locate the object having the override you want to edit by using object filters and search field.
- Step 3** Click the edit icon  in the **Actions** pane.
- Step 4** Modify the override value:
- Click the edit icon to modify the value.
 - Click the cell in the **Devices** column to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
 - Click  arrow in **Default Values** to push and make it an additional value of the shared network group. All devices associated with the shared network group are automatically assigned to it.
 - Click  arrow in **Override Values** to push and make it as default objects of the shared network group.
 - Click the delete icon next to remove the object from the network group.
- Step 5** Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
- Step 6** Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 7 [Preview and Deploy Configuration Changes for All Devices.](#)

Deleting Network Objects and Groups in Security Cloud Control

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Deleting a network object or group from the **Manage > Objects** page deletes the replicated network object or group from the **Manage > Objects** page on the Cloud-Delivered Firewall Management Center and vice-versa.

Create or Edit a Firepower Network Object or Network Groups

A **Firepower network object** can contain a hostname, an IP address, or a subnet address expressed in CIDR notation. **Network groups** are conglomerates of network objects and network groups that are used in access rules, network policies, and NAT rules. You can create, read, update, and delete network objects and network groups using Security Cloud Control.

Firepower network objects and groups can be used by ASA, Firewall Threat Defense, FDM-managed, and Meraki devices. See [Reusing Network Objects Across Products, on page 27](#).



Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.



Caution

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Table 4: IP addresses that can be added to network objects

| Device type | IPv4 / IPv6 | Single Address | Range of addresses | Partially Qualified Domain Name (PQDN) | Subnet using CIDR Notation |
|-------------|-------------|----------------|--------------------|--|----------------------------|
| Firepower | IPv4 / IPv6 | Yes | Yes | Yes | Yes |

Related Information:

- [Create a Firepower Network Object, on page 36](#)

- [Edit a Firepower Network Object, on page 38](#)
- [Add Additional Values to a Shared Network Group, on page 41](#)
- [Edit Additional Values in a Shared Network Group, on page 42](#)

Create a Firepower Network Object




Note

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.

Procedure

Step 1 In the left pane, click **Manage > Objects**.

Step 2 Click the blue plus button  to create an object.

Step 3 Click **FTD > Network**.

Step 4 Enter an **Object Name**.

Step 5 Select **Create a network object**.

Step 6 In the **Value** section:

- Select **eq** and enter a single IP address, a subnet address expressed in CIDR notation, or a Partially Qualified Domain Name (PQDN).
- Select **range** and enter an IP address range.

Note

Do not set a host bit value. If you enter a host bit value other than 0, Security Cloud Control unsets it while creating the object, because the cloud-delivered Firewall Management Center only accepts IPv6 objects with host bits not set.

Step 7 Click **Add**.

Attention: The newly created network objects aren't associated with any FDM-managed device as they aren't part of any rule or policy. To see these objects, select the **Unassociated** objects category in object filters. For more information, see [Object Filters](#). Once you use the unassociated objects in a device's rule or policy, such objects are associated with that device.

Create a Firepower Network Group

A **network group** can contain network objects and network groups. When you create a new network group, you can search for existing objects by their name, IP addresses, IP address range, or FQDN and add them to


the network group. If the object isn't present, you can instantly create that object in the same interface and add it to the network group.



Note If Cloud-Delivered Firewall Management Center is deployed on your tenant:

When you create an FTD, FDM, or ASA network object or group on the **Objects** page, a copy of the object is automatically added to the Cloud-Delivered Firewall Management Center and vice-versa. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the objects to the on-premises management center on which you want these objects.

Procedure

-
- Step 1** In the left pane, click **Manage > Objects**.
- Step 2** Click the blue plus button  to create an object.
- Step 3** Click **FTD > Network**.
- Step 4** Enter an **Object Name**.
- Step 5** Select **Create a network group**.
- Step 6** In the **Values** field, enter a value or name. When you start typing, Security Cloud Control provides object names or values that match your entry.
- Step 7** You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.
- Step 8** If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.
- Step 9** If you have entered a value or object that is not present, you can perform one of the following:
- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
 - Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.
- It is possible to create a new object even though the value is already present. You can make changes to those objects and save them.
- Note:** You can click the edit icon to modify the details. Clicking the delete button doesn't delete the object itself; instead, it removes it from the network group.
- Step 10** After adding the required objects, click **Save** to create a new network group.
- Step 11** [Preview and Deploy Configuration Changes for All Devices](#).
-

Edit a Firepower Network Object



Caution

If Cloud-Delivered Firewall Management Center is deployed on your tenant:


Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Manage > Objects**.

Step 2 Locate the object you want to edit by using object filters and search field.

Step 3 Select the network object and click the edit icon  in the **Actions** pane.

Step 4 Edit the values in the dialog box in the same fashion that you created them in "Create a Firepower Network Group".

Note

Click the delete icon next to remove the object from the network group.

Step 5 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Edit a Firepower Network Group



Caution

If Cloud-Delivered Firewall Management Center is deployed on your tenant:


Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure


Step 1 In the left pane, click **Manage > Objects**.

Step 2 Locate the network group you want to edit by using object filters and search field.

Step 3 Select the network group and click the edit icon  in the **Actions** pane.

Step 4 Change the object name and description if needed.

Step 5 If you want to change the objects or network groups that are already added to the network group, perform the following steps:

- a. Click the edit icon  appearing beside the object name or network group to modify them.
- b. Click the checkmark to save your changes. **Note:** You can click the remove icon to delete the value from a network group.

Step 6 If you want to add new network objects or network groups to this network group, you have to perform the following steps:

- a. In the **Values** field, enter a new value or the name of an existing network object. When you start typing, Security Cloud Control provides object names or values that match your entry. You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.
- b. If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.
- c. If you have entered a value or object that is not present, you can perform one of the following:
 - Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
 - Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.

It's possible to create a new object even though the value is already present. You can make changes to those objects and save them.

Step 7 Click **Save**. Security Cloud Control displays the policies that will be affected by the change.

Step 8 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 9 [Preview and Deploy Configuration Changes for All Devices](#).

Add an Object Override




Caution

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

- Step 1** In the left pane, click **Manage > Objects**.
- Step 2** Locate the object to which you want to add an override, using object filters and search field.
- Step 3** Select the network object and click the edit icon  in the **Actions** pane.
- Step 4** Enter the value in the **Override Values** dialog box and click + **Add Value**.

Important

The override you are adding must have the same type of value that the object contains. For example, to a network object, you can configure an override only with a network value and not a host value.

- Step 5** Once you see that the value is added, click the cell in the **Devices** column in **Override Values**.
- Step 6** Click **Add Devices**, and choose the device to which you want the override to be added. The device you select must contain the object to which you are adding the override.
- Step 7** Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
- Step 8** Click **Confirm** to finalize the addition of the override to the object and any devices affected by it.

Note



You can add more than one override to an object. However, you must select a different device, which contains the object, each time you are adding an override.

- Step 9** See [Object Overrides, on page 20](#) to know more about object overrides and [Edit Object Overrides , on page 40](#) to edit an existing override.

Edit Object Overrides

You can modify the value of an existing override as long as the object is present on the device.

Procedure

- Step 1** Navigate to **Manage > Objects**.
- Step 2** Locate the object having override you want to edit by using object filters and search field.
- Step 3** Select the object having override and click the edit icon  in the **Actions** pane.
- Step 4** Modify the override value:
- Click the edit icon to modify the value.
 - Click on the cell in the **Devices** column in **Override Values** to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
 - Click  arrow in **Override Values** to push and make it as the default value of the shared object.
 - Click the delete icon next to the override you want to remove.
- Step 5** Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 7 [Preview and Deploy Configuration Changes for All Devices.](#)

Add Additional Values to a Shared Network Group

The values in a shared network group that are present on all devices associated with it are called "default values." Security Cloud Control allows you to add "additional values" to the shared network group and assign those values to some devices associated with that shared network group. When Security Cloud Control deploys the changes to the devices, it determines the contents and pushes the "default values" to all devices associated with the shared network group and the "additional values" only to the specified devices.

For example, consider a scenario where you have four AD main servers in your head office that should be accessible from all your sites. Therefore, you have created an object group named "Active-Directory" to use in all your sites. Now you want to add two more AD servers to one of your branch offices. You can do this by adding their details as additional values specific to that branch office on the object group "Active-Directory." These two servers do not participate in determining whether the object "Active-Directory" is consistent or shared. Therefore, the four AD main servers are accessible from all your sites, but the branch office (with two additional servers) can access two AD servers and four AD main servers.



Note

If there are inconsistent shared network groups, you can combine them into a single shared network group with additional values. See [Resolve Inconsistent Object Issues](#) for more information.



Caution

If Cloud-Delivered Firewall Management Center is deployed on your tenant:


Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

Step 1 In the left pane, click **Manage > Objects**.

Step 2 Locate the shared network group you want to edit by using object filters and search field.

Step 3 Click the edit icon  in the **Actions** pane.

- The **Devices** field shows the devices the shared network group is present.
- The **Usage** field shows the rulesets associated with the shared network group.
- The **Default Values** field specifies the default network objects and their values associated with the shared network group that was provided during their creation. Next to this field, you can see the number of devices that contain

this default value, and you can click to see their names and device types. You can also see the rulesets associated with this value.

- Step 4** In the **Additional Values** field, enter a value or name. When you start typing, Security Cloud Control provides object names or values that match your entry.
- Step 5** You can choose one of the existing objects shown or create a new one based on the name or value that you have entered.
- Step 6** If Security Cloud Control finds a match, to choose an existing object, click **Add** to add the network object or network group to the new network group.
- Step 7** If you have entered a value or object that is not present, you can perform one of the following:
- Click **Add as New Object With This Name** to create a new object with that name. Enter a value and click the checkmark to save it.
 - Click **Add as New Object** to create a new object. The object name and value are the same. Enter a name and click the checkmark to save it.
- It is possible to create a new object even though the value is already present. You can make changes to those objects and save them.
- Step 8** In the **Devices** column, click the cell associated with the newly added object and click **Add Devices**.
- Step 9** Select the devices that you want and click **OK**.
- Step 10** Click **Save**. Security Cloud Control displays the devices that will be affected by the change.
- Step 11** Click **Confirm** to finalize the change to the object and any devices affected by it.
- Step 12** [Preview and Deploy Configuration Changes for All Devices](#).

Edit Additional Values in a Shared Network Group




Caution



If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Changes you make to the ASA, FDM, and FTD network objects and groups are reflected in the corresponding Cloud-Delivered Firewall Management Center network object or group. In addition, an entry is created in the **Devices with Pending Changes** page for each on-premises management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises management center on which you have these objects.

Deleting a network object or group from either page deletes the object or group from both pages.

Procedure

- Step 1** In the left pane, click **Manage > Objects**.
- Step 2** Locate the object having the override you want to edit by using object filters and search field.
- Step 3** Click the edit icon  in the **Actions** pane.
- Step 4** Modify the override value:
- Click the edit icon to modify the value.

- Click the cell in the **Devices** column to assign new devices. You can select an already assigned device and click **Remove Overrides** to remove overrides on that device.
- Click  arrow in **Default Values** to push and make it an additional value of the shared network group. All devices associated with the shared network group are automatically assigned to it.
- Click  arrow in **Override Values** to push and make it as default objects of the shared network group.
- Click the delete icon next to remove the object from the network group.

Step 5 Click **Save**. Security Cloud Control displays the devices that will be affected by the change.

Step 6 Click **Confirm** to finalize the change to the object and any devices affected by it.

Step 7 [Preview and Deploy Configuration Changes for All Devices](#).

Deleting Network Objects and Groups in Security Cloud Control

If Cloud-Delivered Firewall Management Center is deployed on your tenant:

Deleting a network object or group from the **Manage > Objects** page deletes the replicated network object or group from the **Manage > Objects** page on the Cloud-Delivered Firewall Management Center and vice-versa.

Discover and Manage On-Prem Firewall Management Center Network Objects

If you have an On-Premises Firewall Management Center that you manage using Security Cloud Control and you want to share and manage its objects, do the following:

Procedure

Step 1 In the left pane, choose **Administration > Integrations > Firewall Management Center** to view the **Services** page.

Step 2 If you already have onboarded an on-premises management center to Security Cloud Control, select it.

If you want to onboard a new on-premises management center, see [Onboard an On-Prem Firewall Management Center](#).

Step 3 Choose **Settings** from the **Actions** pane on the right. Note that you do not get to see the **Actions** pane when you select more than one on-premises management center.

Note

You must be an admin or a super admin to be able to use **Settings**.

Step 4 Enable the **Discover & Manage Network Objects** toggle button. If you want your changes to be automatically synchronized with on-premises management center and not staged for review, turn the **Enable automatic sync of network objects** toggle on.

Note

- You cannot turn the **Discover & Manage Network Objects** toggle on if the on-premises management center that you have selected has one or more child domains or has the Change Management workflow enabled on it.
- You cannot turn the **Enable automatic sync of network objects** toggle on if the **Discover & Manage Network Objects** toggle is turned off.

For every new on-premises management center onboarded to Security Cloud Control, this toggle button needs to be enabled manually. Once you enable this option, Security Cloud Control starts to discover objects from your on-premises management center, which you can share, manage, and use to set consistent object definitions across other platforms managed by Security Cloud Control.

In Security Cloud Control, when you add overrides to objects that are discovered from an on-premises management center and push the changes back to the on-premises management center, these objects start accepting overrides in the on-premises management center even if they were not accepting overrides before—the **Allow Overrides** checkbox in **View Network Object** window is checked automatically when an override is added from Security Cloud Control.

Note

If you want to assign already-existing objects in Security Cloud Control to your on-premises management center, choose the on-premises management center and click **Assign Objects** from the **Actions** pane.

Related Information

- [Network Objects](#)
- [Preview and Deploy On-Prem Firewall Management Center Configurations](#)
- [Enable Conflict Detection for an On-Premises Management Center](#)

Service Objects

Protocol Objects

Protocol objects are a type of service object that contain less-commonly used or legacy protocols. Protocol objects are identified by a name and [protocol number](#). Security Cloud Control recognizes these objects in ASA and Firepower (FDM-managed device) configurations and gives them their own filter of "Protocols" so you can find them easily.

ICMP Objects

An Internet Control Message Protocol (ICMP) object is a service object specifically for ICMP and IPv6-ICMP messages. Security Cloud Control recognizes these objects in ASA and Firepower configurations when those devices are onboarded and Security Cloud Control gives them their own filter of "ICMP" so you can find the objects easily.

Using Security Cloud Control, you can rename or remove ICMP objects from an ASA configuration. You can use Security Cloud Control to create, update, and delete ICMP and ICMPv6 objects in a Firepower configuration.



Note For the ICMPv6 protocol, AWS does not support choosing specific arguments. Only rules that allow all ICMPv6 messages are supported.

Related Information:

- [Deleting Objects, on page 25](#)

Network Address Translation

Each computer and device within an IP network is assigned a unique IP address that identifies the host. Because of a shortage of public IPv4 addresses, most of these IP addresses are private and not routable anywhere outside of the private company network. RFC 1918 defines the private IP addresses you can use internally that should not be advertised:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

One of the main functions of Network Address Translation (NAT) is to enable private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses because it can be configured to advertise at a minimum only one public address for the entire network to the outside world.

Other functions of NAT include:

- Security-Keeping internal IP addresses hidden discourages direct attacks.
- IP routing solutions-Overlapping IP addresses are not a problem when you use NAT.
- Flexibility-You can change internal IP addressing schemes without affecting the public addresses available externally; for example, for a server accessible to the Internet, you can maintain a fixed IP address for Internet use, but internally, you can change the server address.
- Translating between IPv4 and IPv6 (Routed mode only)-If you want to connect an IPv6 network to an IPv4 network, NAT lets you translate between the two types of addresses.

You can use Security Cloud Control to create NAT rules for many different use cases. Use the NAT rule wizard or these topics to create different NAT rules:

Order of Processing NAT Rules

Network Object NAT and twice NAT rules are stored in a single table that is divided into three sections. Section 1 rules are applied first, then section 2, and finally section 3, until a match is found. For example, if a match is found in section 1, sections 2 and 3 are not evaluated. The following table shows the order of rules within each section.

Table 5: NAT Rule Table

| Table Section | Rule Type | Order of Rules within the Section |
|---------------|-------------------------------------|---|
| Section 1 | Twice NAT (ASA) Manual NAT (FTD) | Applied on a first match basis, in the order they appear in the configuration. Because the first match is applied, you must ensure that specific rules come before more general rules, or the specific rules might not be applied as desired. By default, twice NAT rules are added to section 1. |

| Table Section | Rule Type | Order of Rules within the Section |
|---------------|--|---|
| Section 2 | Network Object NAT (ASA) Auto NAT (FTD) | <p>If a match in section 1 is not found, section 2 rules are applied in the following order:</p> <ol style="list-style-type: none"> 1. Static rules. 2. Dynamic rules. <p>Within each rule type, the following ordering guidelines are used:</p> <ol style="list-style-type: none"> 1. Quantity of real IP addresses—From smallest to largest. For example, an object with one address will be assessed before an object with 10 addresses. 2. For quantities that are the same, then the IP address number is used, from lowest to highest. For example, 10.1.1.0 is assessed before 11.1.1.0. 3. If the same IP address is used, then the name of the network object is used, in alphabetical order. For example, object "Arlington" is assessed before object "Detroit." |
| Section 3 | Twice NAT (ASA) Manual NAT (FTD) | <p>If a match is still not found, section 3 rules are applied on a first match basis, in the order they appear in the configuration. This section should contain your most general rules. You must also ensure that any specific rules in this section come before general rules that would otherwise apply.</p> |

For section 2 rules, for example, you have the following IP addresses defined within network objects:

- 192.168.1.0/24 (static)
- 192.168.1.0/24 (dynamic)
- 10.1.1.0/24 (static)
- 192.168.1.1/32 (static)
- 172.16.1.0/24 (dynamic) (object Detroit)
- 172.16.1.0/24 (dynamic) (object Arlington)

The resultant ordering would be:

- 192.168.1.1/32 (static)
- 10.1.1.0/24 (static)
- 192.168.1.0/24 (static)
- 172.16.1.0/24 (dynamic) (object Arlington)

- 172.16.1.0/24 (dynamic) (object Detroit)
- 192.168.1.0/24 (dynamic)

Network Address Translation Wizard

The Network Address Translation (NAT) wizard helps you create NAT rules on your devices for these types of access:

- **Enable Internet Access for Internal Users.** You may use this NAT rule to allow users on an internal network to reach the internet.
- **Expose an Internal Server to the Internet.** You may use this NAT rule to allow people outside your network to reach an internal web or email server.

Prerequisites to "Enable Internet Access for Internal Users"

Before you create your NAT rule, gather this information:

- The interface that is closest to your users; this is usually called the "inside" interface.
- The interface closest to your Internet connection; this is usually called the "outside" interface.
- If you want to allow only specific users to reach the internet, you need the subnet addresses for those users.

Prerequisites to "Expose an Internal Server to the Internet"

Before you create your NAT rule, gather this information:

- The interface that is closest to your users; this is usually called the "inside" interface.
- The interface closest to your Internet connection; this is usually called the "outside" interface.
- The IP address of the server inside your network that you would like to translate to an internet-facing IP address.
- The public IP address you want the server to use.

What to do Next




See [Create a NAT Rule by using the NAT Wizard, on page 47](#).

Create a NAT Rule by using the NAT Wizard

Before you begin

See [Network Address Translation Wizard, on page 47](#) for the prerequisites needed to create NAT rules using the NAT wizard.

Procedure

-
- Step 1** In the left pane, click **Security Devices**.
- Step 2** Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
- Step 3** Click the appropriate device type tab.
- Step 4** Use the filter ([filter](#)) and search ([search](#)) fields to find the device for which you want to create the NAT rule.
- Step 5** In the **Management** area of the details panel, click **NAT**  **NAT**.
- Step 6** Click  **> NAT Wizard**.
- Step 7** Respond to the NAT Wizard questions and follow the on-screen instructions.
- The NAT Wizard creates rules with [Network Objects, on page 26](#). Either select an existing object from the drop-down menu, or create a new object with the create button  **Create...**.
 - Before you can save the NAT rule, all IP addresses need to be defined as network objects.
- Step 8** [Review and deploy](#) now the changes you made, or wait and deploy multiple changes at once.
-

Common Use Cases for NAT

Twice NAT and Manual NAT

Here are some common tasks that can be achieved using "Network Object NAT", also known as "Auto NAT":

- [Enable a Server on the Inside Network to Reach the Internet Using a Public IP address, on page 48](#)
- [Enable Users on the Inside Network to Access the Internet Using the Outside Interface's Public IP Address, on page 50](#)
- [Make a Server on the Inside Network Available on a Specific Port of a Public IP Address, on page 51](#)
- [Translate a Range of Private IP Addresses to a Range of Public IP Addresses, on page 54](#)

Network Object NAT and Auto NAT

Here is a common task that can be achieved using "Twice NAT", also known as "Manual NAT":

- [Prevent a Range of IP Addresses from Being Translated When Traversing the Outside Interface, on page 55](#)

Enable a Server on the Inside Network to Reach the Internet Using a Public IP address

Use Case

Use this NAT strategy when you have a server with a private IP address that needs to be accessed from the internet and you have enough public IP addresses to NAT one public IP address to the private IP address. If you have a limited number of public IP addresses, see [Make a server on the inside network available to users on a specific port of a public IP address](#) (that solution may be more suitable).

Strategy


Your server has a static, private IP address, and users outside your network have to be able to reach your server. Create a network object NAT rule that translates the static private IP address to a static public IP address. After that, create an access policy that allows traffic from that public IP address to reach the private IP address. Finally, deploy these changes to your device.

Before you begin

Before you begin, create two network objects. Name one object *servername_inside* and the other object *servername_outside*. The *servername_inside* network object should contain the private IP address of your server. The *servername_outside* network object should contain the public IP address of your server.

See [Create Network Objects](#) for instructions.

Procedure

-
- | | |
|----------------|---|
| Step 1 | In the left pane, click Security Devices . |
| Step 2 | Click the Devices tab to locate the device or the Templates tab to locate the model device. |
| Step 3 | Click the appropriate device type tab. |
| Step 4 | Select the device you want to create the NAT rule for. |
| Step 5 | Click NAT in the Management pane at the right. |
| Step 6 | Click  > Network Object NAT . |
| Step 7 | In section 1, Type , select Static . Click Continue . |
| Step 8 | In section 2, Interfaces , choose inside for the source interface and outside for the destination interface. Click Continue . |
| Step 9 | In section 3, Packets , perform these actions: <ol style="list-style-type: none"> a. Expand the Original Address menu, click Choose, and select the servername_inside object. b. Expand the Translated Address menu, click Choose, and select the servername_outside object. |
| Step 10 | Skip section 4, Advanced . |
| Step 11 | For an FDM-managed device, in section 5, Name , give the NAT rule a name. |
| Step 12 | Click Save . |
| Step 13 | For ASA, deploy a Network Policy rule or for FDM-managed device, deploy an access control policy rule to allow the traffic to flow from <i>servername_inside</i> to <i>servername_outside</i> . |
| Step 14 | Review and deploy now the changes you made, or wait and deploy multiple changes at once. |
-

Enable Users on the Inside Network to Access the Internet Using the Outside Interface's Public IP Address

Use Case


Allow users and computers in your private network to connect to the internet by sharing the public address of your outside interface.

Strategy

Create a port address translation (PAT) rule that allows all the users on your private network to share the outside interface public IP address of your device.

After the private address is mapped to the public address and port number, the device records that mapping. When incoming traffic bound for that public IP address and port is received, the device sends it back to the private IP address that requested it.

Procedure

-
- Step 1** In the left pane, click **Security Devices**.
- Step 2** Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
- Step 3** Click the appropriate device type tab.
- Step 4** Select the device you want to create the NAT rule for.
- Step 5** Click **NAT** in the **Management** pane at the right.
- Step 6** Click  **Network Object NAT**.
- Step 7** In section 1, **Type**, select **Dynamic**. Click **Continue**.
- Step 8** In section 2, **Interfaces**, choose **any** for the source interface and **outside** for the destination interface. Click **Continue**.
- Step 9** In section 3, **Packets**, perform these actions :
- Expand the Original Address menu, click **Choose** and select the **any-ipv4** or **any-ipv6** object depending on your network configuration.
 - Expand the Translated Address menu, and select **interface** from the available list. Interface indicates to use the public address of the outside interface.
- Step 10** For an FDM-managed device, in section 5, **Name**, enter a name for the NAT rule.
- Step 11** Click **Save**.
- Step 12** [Review and deploy](#) now the changes you made, or wait and deploy multiple changes at once.
-

Entries in the ASA's Saved Configuration File

Here are the entries that are created and appear in an ASA's saved configuration file as a result of this procedure.



Note This does not apply to FDM-managed devices.

Objects created by this procedure:

```
object network any_network
subnet 0.0.0.0 0.0.0.0
```

NAT rules created by this procedure:

```
object network any_network
nat (any,outside) dynamic interface
```

Make a Server on the Inside Network Available on a Specific Port of a Public IP Address

Use Case

If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.


Prerequisites

Before you begin, create three separate network objects, one each for an FTP, HTTP, and SMTP server. For the sake of the following procedures, we call these objects **ftp-server-object**, **http-server-object**, and **smtp-server-object**.

See for instructions.

NAT Incoming FTP Traffic to an FTP Server

Procedure

-
- Step 1** In the left pane, click **Security Devices**.
 - Step 2** Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
 - Step 3** Click the appropriate device type tab.
 - Step 4** Select the device you want to create the NAT rule for.
 - Step 5** Click **NAT** in the **Management** pane at the right.
 - Step 6** Click  > **Network Object NAT**.
 - Step 7** In section 1, **Type**, select **Static**. Click **Continue**.
 - Step 8** In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.
 - Step 9** In section 3, **Packets**, perform these actions:
 - Expand the Original Address menu, click **Choose**, and select the **ftp-server-object**.
 - Expand the Translated Address menu, click **Choose**, and select the **Interface**.
 - Check **Use Port Translation**.
 - Select **tcp, ftp, ftp**.



- Step 10** Skip section 4, **Advanced**.
- Step 11** For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.
- Step 12** Click **Save**. The new rule is created in [section 2](#) of the NAT table.
- Step 13** [Review and deploy](#) now the changes you made, or wait and deploy multiple changes at once.

NAT Incoming HTTP Traffic to an HTTP Server


If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Before you begin

Before you begin, create a network object for the http server. For the sake of this procedure, we will call the object, **http-object**.

See for instructions.

Procedure

- Step 1** In the left pane, click **Security Devices**.
- Step 2** Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
- Step 3** Click the appropriate device type tab.
- Step 4** Select the device you want to create the NAT rule for.
- Step 5** Click **NAT** in the **Management** pane at the right.
- Step 6** Click  > **Network Object NAT**.
- Step 7** In section 1, **Type**, select **Static**. Click **Continue**.
- Step 8** In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.
- Step 9** In section 3, **Packets**, perform these actions:
- Expand the Original Address menu, click **Choose**, and select the **http-object**.
 - Expand the Translated Address menu, click **Choose**, and select the **Interface**.
 - Check **Use Port Translation**.
 - Select **tcp**, **http**, http.



- Step 10** Skip section 4, **Advanced**.

- Step 11** For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.
- Step 12** Click **Save**. The new rule is created in [section 2](#) of the NAT table.
- Step 13** [Review and deploy](#) now the changes you made, or wait and deploy multiple changes at once.

NAT Incoming SMTP Traffic to an SMTP Server


If you only have one public IP address, or a very limited number, you can create a network object NAT rule that translates inbound traffic, bound for a static IP address and port, to an internal address. We have provided procedures for specific cases, but you can use them as a model for other supported applications.

Before you begin

Before you begin, create a network object for the smtp server. For the sake of this procedure, we will call the object, **smtp-object**.

See for instructions.

Procedure

- Step 1** In the left pane, click **Security Devices**.
- Step 2** Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
- Step 3** Click the appropriate device type tab.
- Step 4** Select the device you want to create the NAT rule for.
- Step 5** Click **NAT** in the **Management** pane at the right.
- Step 6** Click  > **Network Object NAT**.
- Step 7** In section 1, **Type**, select **Static**. Click **Continue**.
- Step 8** In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.
- Step 9** In section 3, **Packets**, perform these actions:
- Expand the Original Address menu, click **Choose**, and select the smtp-server-object.
 - Expand the Translated Address menu, click **Choose**, and select the **Interface**.
 - Check **Use Port Translation**.
 - Select **tcp**, **smtp**, **smtp**.
-
- Step 10** Skip section 4, **Advanced**.
- Step 11** For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.
- Step 12** Click **Save**. The new rule is created in [section 2](#) of the NAT table.
- Step 13** [Review and deploy](#) now the changes you made, or wait and deploy multiple changes at once.

Translate a Range of Private IP Addresses to a Range of Public IP Addresses

Use Case

Use this approach if you have a group of specific device types, or user types, that need to have their IP addresses translated to a specific range so that the receiving devices (the devices on the other end of the transaction) allow the traffic in.

Translate a Pool of Inside Addresses to a Pool of Outside Addresses

Before you begin

Create a network object for the pool of private IP addresses you want to translate and create a network object for the pool of public addresses you want to translate those private IP addresses into.




Note For the ASA, the network group that defines the pool of "translated address" cannot be a network object that defines a subnet.

When creating these address pools, for instructions.

For the sake of the following procedure, we named the pool of private addresses, **inside_pool** and name the pool of public addresses, **outside_pool**.

Procedure

- Step 1** In the left pane, click **Security Devices**.
- Step 2** Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
- Step 3** Click the appropriate device type tab.
- Step 4** Select the device you want to create the NAT rule for.
- Step 5** Click **NAT** in the **Management** pane at the right.
- Step 6** Click  > **Network Object NAT**.
- Step 7** In section 1, **Type**, select **Dynamic** and click **Continue**.
- Step 8** In section 2, **Interfaces**, set the source interface to **inside** and the destination interface to **outside**. Click **Continue**.
- Step 9** In section 3, **Packets**, perform these tasks:
 - For the Original Address, click **Choose** and then select the **inside_pool** network object (or network group) you made in the prerequisites section above.
 - For the Translated Address, click **Choose** and then select the **outside_pool** network object (or network group) you made in the prerequisites section above.
- Step 10** Skip section 4, **Advanced**.
- Step 11** For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.
- Step 12** Click **Save**.

Step 13 [Review and deploy](#) now the changes you made, or wait and deploy multiple changes at once.

Prevent a Range of IP Addresses from Being Translated When Traversing the Outside Interface

Use Case

Use this Twice NAT use case to enable site-to-site VPN.

Strategy

You are translating a pool of IP addresses to itself so that the IP addresses in one location on the network arrives unchanged in another.

Create a Twice NAT Rule


Before you begin

Create a network object or network group that defines the pool of IP addresses you are going to translate to itself. For the ASA, the range of addresses can be defined by a network object that uses an IP address range, a network object that defines a subnet, or a network group object that includes all the addresses in the range.

When creating the network objects or network groups, use for instructions.

For the sake of the following procedure, we are going call the network object or network group, Site-to-Site-PC-Pool.

Procedure

- Step 1** In the left pane, click **Security Devices**.
- Step 2** Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
- Step 3** Click the appropriate device type tab.
- Step 4** Select the device you want to create the NAT rule for.
- Step 5** Click **NAT** in the **Management** pane at the right.
- Step 6** Click  > **Twice NAT**.
- Step 7** In section 1, **Type**, select **Static**. Click **Continue**.
- Step 8** In section 2, **Interfaces**, choose **inside** for the source interface and **outside** for the destination interface. Click **Continue**.
- Step 9** In section 3, **Packets**, make these changes:
- Expand the Original Address menu, click **Choose**, and select the Site-to-Site-PC-Pool object you created in the prerequisites section.
 - Expand the Translated Address menu, click **Choose**, and select the Site-to-Site-PC-Pool object you created in the prerequisites section.

- Step 10** Skip section 4, **Advanced**.
- Step 11** For an FDM-managed device, in section 5, **Name**, give the NAT rule a name.
- Step 12** Click **Save**.
- Step 13** For an ASA, create a crypto map. See [CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide](#) and review the chapter on LAN-to-LAN IPsec VPNs for more information on creating a crypto map.
- Step 14** [Review and deploy](#) now the changes you made, or wait and deploy multiple changes at once.
-