Manage objects

This chapter describes how to create and manage reusable objects.

Introduction to objects

An object is a reusable container of information that you can use in one or more security policies. Objects help you maintain policy consistency because you can define a value once, use it in multiple policies, and update every policy that uses the object by changing the object.

When you onboard a device, Security Cloud Control Firewall Management 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 Firewall Management calls an object used on multiple devices a **shared object** and identifies them in the **Objects** page with this badge .

You can use Security Cloud Control Firewall Management to manage objects in these ways:

- Search for and filter all your objects based on a variety of criteria.
- Find duplicate, unused, and inconsistent objects, and then consolidate, delete, resolve, ignore, or unignore object issues.
- Find and delete unassociated objects if they are not needed.
- Discover objects that are shared across devices.
- Evaluate which policies and devices are affected before you commit an object change.
- Compare a set of objects and their relationships with different policies and devices.
- Capture objects that are in use after a device is onboarded to Security Cloud Control Firewall Management.

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

- **Duplicate objects**: Two or more objects on the same device have 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**: Two or more devices have objects with the same name but different values. This issue can occur when objects start with the same name and content but later diverge. Inconsistent objects are identified by this issue icon:
- **Unused objects**: An object exists in a device configuration but is 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 Firewall Management creates a copy of it and uses the copy.

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

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

Supported object types

The object types that you can create and manage depend on the managed device type.

Common object types

Table 1: Common Objects

Object Type	Description
Network	Network groups and network objects (collectively referred to as network objects) define the addresses of hosts or networks.
URL	Use URL objects and groups (collectively referred to as URL objects) to define the URL or IP addresses of web requests. You can use these objects to implement manual URL filtering in access control policies or blocking in Security Intelligence policies.

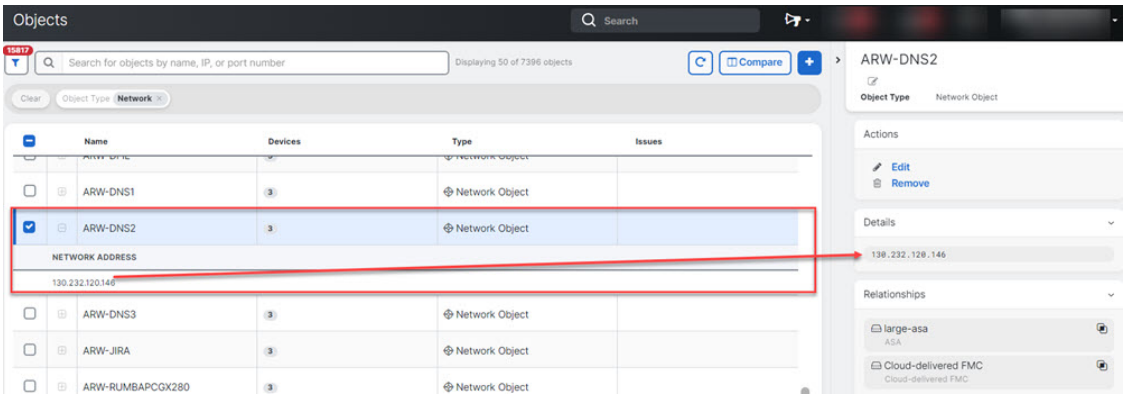
Shared objects

A shared object is an object on multiple devices that has the same name and the same contents. Shared objects help you maintain policies because one object change affects every policy that uses that shared object.

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 lets you customize a shared object for specific devices. When a device has an override, Security Cloud Control Firewall Management uses the override value for that device instead of the object's default value.

Overrides allow you to maintain a single shared policy across devices while tailoring individual object values where needed.

Use overrides when you want to maintain one shared policy across devices but need specific devices to use different object values. For example, a shared print-server object can use the default value 10.1.1.100 for most offices, while Office B uses an override value of 10.2.1.100.

Overrides on network object groups

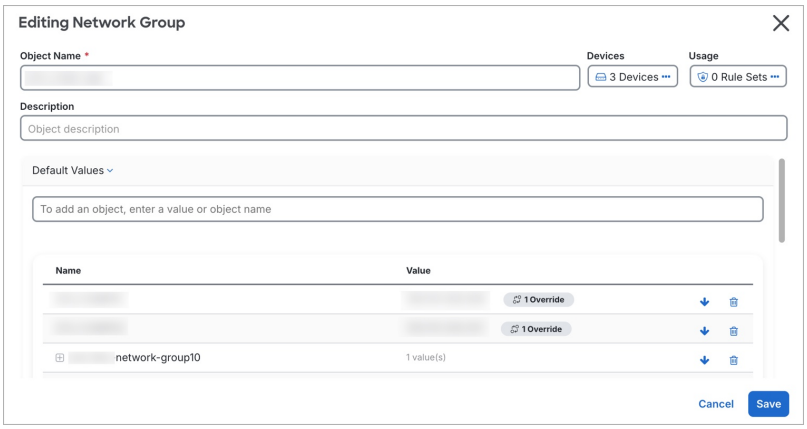
For network object groups, overrides fully replace the default values for the devices that are assigned to the override. A device with an override receives only the override values, not the default values.

This replacement behavior has these effects:

- Changes to default values affect only devices without overrides.
- Changes to an override affect only the devices assigned to that override.
- If a device needs the default values plus a local value, add all required values to the override.

For example, a shared dns-servers network group contains default values primary-dns (10.0.1.53) and secondary-dns (10.0.2.53) for Branch A, Branch B, and Branch C. Branch C also needs local-dns-cache (10.30.1.53). Because a network group override replaces the defaults, the Branch C override must contain primary-dns, secondary-dns, and local-dns-cache.

If you later add a default value, such as tertiary-dns, Branch A and Branch B receive the new default value automatically. Branch C does not receive it until you add tertiary-dns to the Branch C override.



Unassociated objects

An unassociated object is not associated with any rule or policy. When you use an unassociated object in a rule or policy, Security Cloud Control Firewall Management creates and uses a copy of that object. The original unassociated object remains available until a nightly maintenance job deletes it or you delete it manually.

Security Cloud Control Firewall Management keeps unassociated objects as a copy so that configuration data is not lost if the related rule or policy is deleted accidentally.

To view unassociated objects, choose **Objects** > , and check **Unassociated**.

Compare objects

Use object comparison to review up to three objects side by side and inspect their details and relationships.

Procedure

Step 1 From the Security Cloud Control Home page, click **Firewall**.

Step 2 In the left pane, click **Objects** and choose an option.

Step 3 Filter the objects on the page to find the objects you want to compare.

Step 4 Click the **Compare** button Compare.

Step 5 Select up to three objects.

Step 6 Review the objects side-by-side at the bottom of the screen.

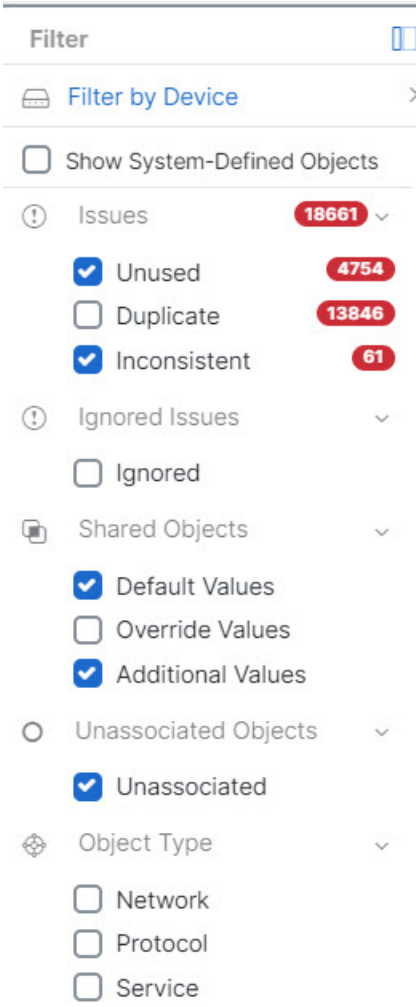
Step 7 (Optional) In **Relationships**, select a device name, and then select **View Configuration** to view the device configuration with the object entry highlighted.

Object filters

Use filters on the **Objects** page to find objects by device, issue, shared state, association state, object type, or search value. You can also include or exclude system-defined objects.

The object type filter lets you filter by object types such as network object, network group, URL object, URL group, service object, and service group. The shared objects filter lets you filter objects that have default values, override values, or additional values.

You can combine device and object filters to create focused search strategies. For example, you can search for objects that match this logic: **Issues** is **Unused** OR **Inconsistent**, AND **Shared Objects** has **Default Values** OR **Additional Values**, AND **Unassociated Objects** is selected.



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

- **Filter by Device**: Shows objects found on selected devices.
- **Show System-Defined Objects**: Includes predefined system objects in search and filter results. System objects cannot be edited or deleted. 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.

- **Issues**: Shows unused, duplicate, or inconsistent objects. If you select more than one issue, objects in any selected issue category are included.
- **Ignored Issues**: Shows objects whose issues were ignored by an administrator.
- **Shared Objects**: Shows shared objects. You can filter by default values, override values, additional values, or a combination.
- **Unassociated Objects**: Shows objects that are not associated with any rule or policy.
- **Object Type**: Shows selected object types, such as network objects, network groups, URL objects, URL groups, service objects, and service groups.

Within a main filter, subfilters can further narrow the results by object type, such as Network, Service, or Protocol. Filters across categories combine with an AND relationship. Multiple selections within a category can combine with an OR relationship.

For example, a filter set can search for objects that match this logic: objects on selected devices AND inconsistent objects AND network objects or service objects AND object names that contain **group**.

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 From the Security Cloud Control Home page, click **Firewall**.

Step 2 In the left pane, click **Objects**.

Step 3 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.

Step 4 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 5 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 6 Check the object **Issues** you want to filter. If you check more than one issue, objects in any of the categories you check are included in your filter results.

Step 7 Check **Ignored** issues if you want to see the object that had issues but was ignored by the administrator.

Step 8 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 9 Check **Unassociated** if you are filtering for objects that are not part of any rule or policy.

Step 10 Check the **Object Types** you want to filter.

Step 11 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.

Exclude device filters when you need full relationships

When you filter by device, Security Cloud Control Firewall Management shows objects on that device but does not show the object's relationships to all other devices.

For example, if ObjectA is shared between ASA1 and ASA2, and you filter for shared objects on ASA1, Security Cloud Control Firewall Management shows `ObjectA`, but the **Relationships** pane shows only that ObjectA is on ASA1.

To view every device and policy relationship for an object, do not specify a device in the filter criteria. Filter by other criteria, select the object, and review the **Relationships** pane.

Unignore objects

Unignore Objects refers to the process of reversing the action of ignoring certain objects that have been marked as unused, duplicate, or inconsistent. Ignoring objects is a way to temporarily leave unresolved issues with these objects when there are valid reasons. However, if you later decide to address these ignored objects, you can unignore them to bring them back into view and take action.

Procedure

Step 1 From the Security Cloud Control Home page, click **Firewall**.

Step 2 In the left pane, click **Objects** and choose an option.

Step 3 Filter and search for ignored objects.

Step 4 In the **Object** table, select the object you want to unignore. You can unignore one object at a time.

Step 5 Click **Unignore** in the details pane.

Step 6 Confirm your request. Now, when you filter your objects by issue, you should find the object that was previously ignored.

Delete objects

You can delete a single object or mulitple objects.

Delete a single object

Note 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 Firewall Management Center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-premises Firewall 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 From the Security Cloud Control Home page, click **Firewall**.

Step 2 In the left pane, click **Objects**.

Step 3 Locate the object you want to delete by using object filters and the search field, and select it.

Step 4 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 5 In the **Actions** pane, click the **Remove** icon .

Step 6 Confirm that you want to delete the object by clicking **OK**.

Step 7 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**.

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

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

Reuse 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 Firewall 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 Firewall 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 Firewall 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.

The following exceptions apply:

- 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 Firewall Management Center is not automatically enabled on Security Cloud Control for new on-premises Firewall Management Centers onboarded to Security Cloud Control. If your network objects are not being shared with On-Premises Firewall Management Center, ensure the **Discover & Manage Network Objects** toggle button is enabled for the on-premises Firewall Management Center in **Settings** or contact TAC to have the features enabled on your tenant.

Viewing network objects

Network objects that you create in Security Cloud Control Firewall Management, and network objects that Security Cloud Control Firewall Management recognizes in onboarded device configurations, appear 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, the **Details** pane shows the object values. The **Relationships** pane shows whether the object is used in a policy and which device stores the object.

When you select a network group, Security Cloud Control Firewall Management shows the contents of the group as the combined values from the network objects in that group.

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:

- Delete objects, on page 7