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, CDO 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.

CDO 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.

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

CDO allows you to manage network and service objects across supported devices from one location. With CDO, 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 CDO.

If you have issues with creating, editing, or reading objects from an onboarded device, see Troubleshoot Cisco Defense Orchestrator for more information.

- Objects, on page 2
- Manage Security Policies in CDO, on page 20
- Meraki Templates, on page 21
- About Device Configuration Changes, on page 22
- Read All Device Configurations, on page 23
- Preview and Deploy Configuration Changes for All Devices, on page 24
- Deploy Changes to a device, on page 25
- Bulk Deploy Device Configurations, on page 25
- About Scheduled Automatic Deployments, on page 26
- Check for Configuration Changes, on page 28
- Discard Configuration Changes, on page 29
- Out-of-Band Changes on Devices, on page 29
- Synchronizing Configurations Between Defense Orchestrator and Device, on page 30
- Conflict Detection, on page 31
- Automatically Accept Out-of-Band Changes from your Device, on page 31
- Resolve Configuration Conflicts, on page 32
- Schedule Polling for Device Changes, on page 34

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, CDO 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.

CDO 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.

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

CDO allows you to manage network and service objects across supported devices from one location. With CDO, 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 CDO.

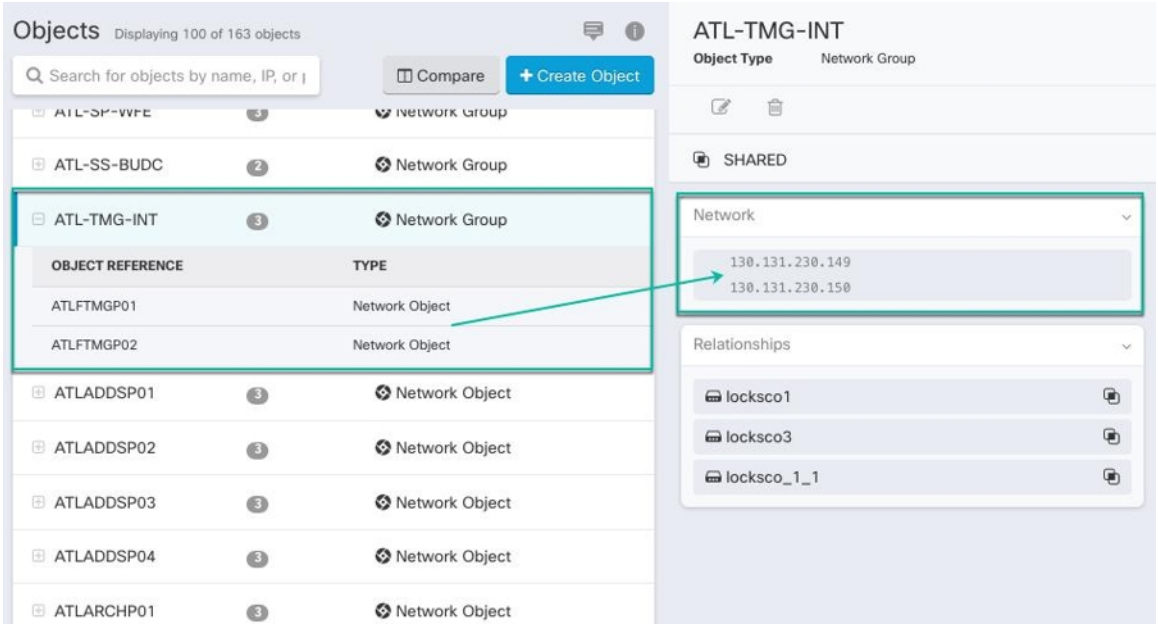
If you have issues with creating, editing, or reading objects from an onboarded device, see Troubleshoot Cisco Defense Orchestrator for more information.

Shared Objects

Cisco Defense Orchestrator (CDO) 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, CDO shows you the contents of the object in the object table. Shared objects have exactly the same contents. CDO 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.

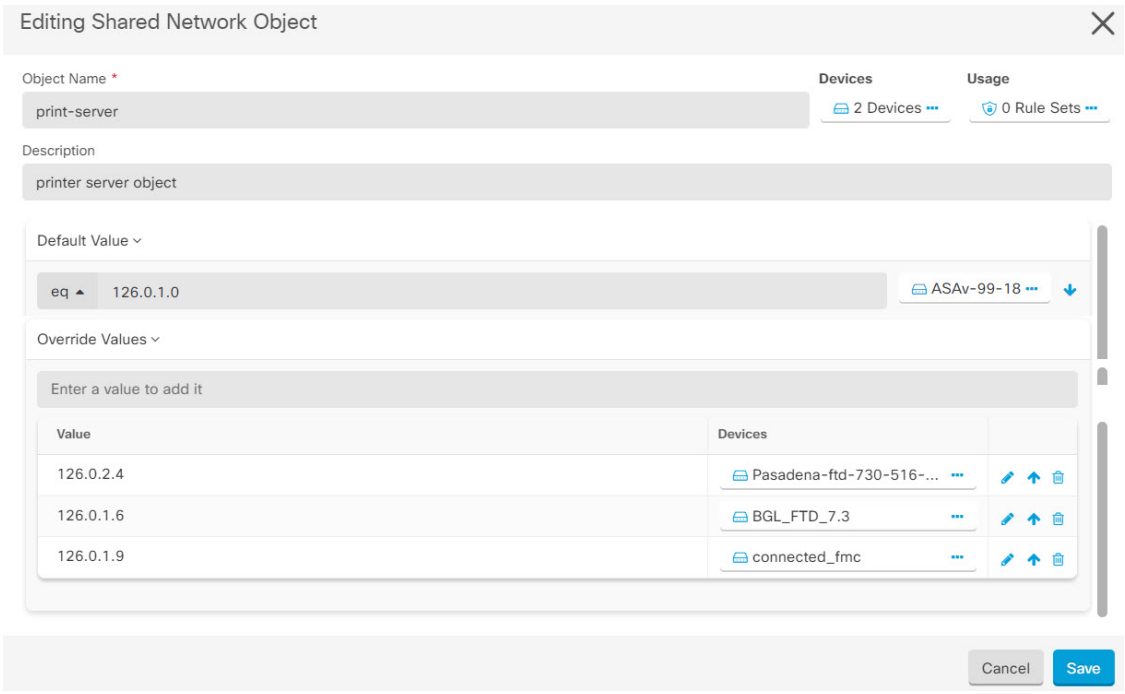


Object Overrides

An object override allows you to override the value of a shared network object on specific devices. CDO 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, CDO 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.



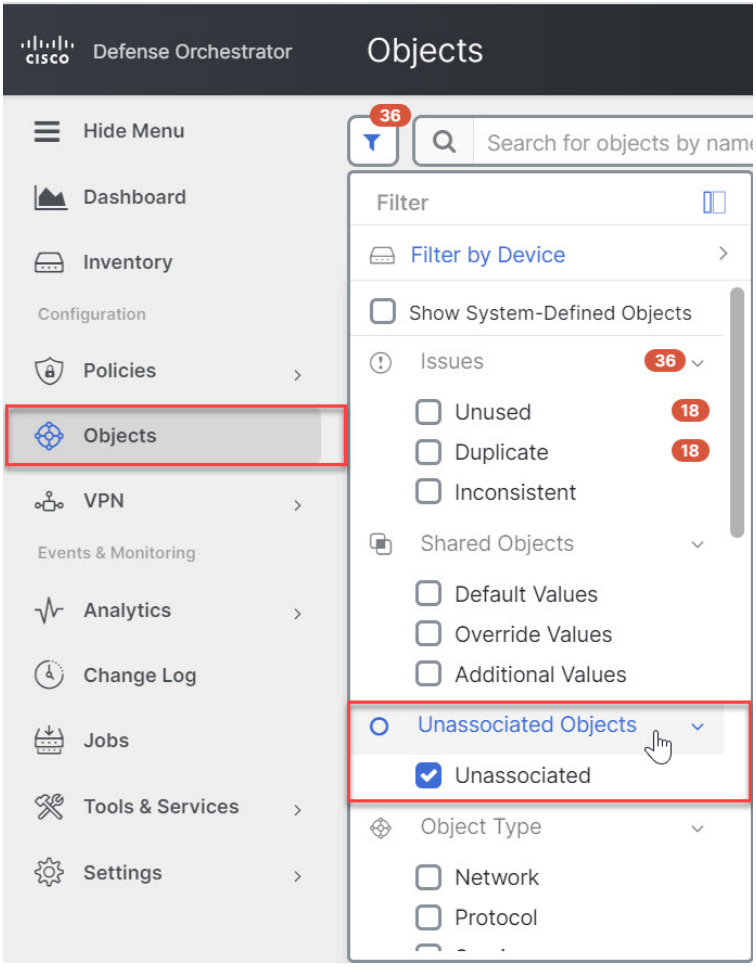
Note If there are inconsistent objects, you can combine them into a single shared object with overrides. See Resolve Inconsistent Object Issues for more information.

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, CDO 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 CDO as a copy to ensure that not all configurations are lost if the rule or policy associated with the object is deleted accidentally.

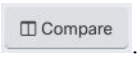
To view unassociated objects click in the left-hand pane of the Objects tab and check the **Unassociated** checkbox.



Compare Objects

Step 1 In the CDO navigation bar on the left, 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. CDO shows you the device's configuration file and highlights the entry for that object.

Filters

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

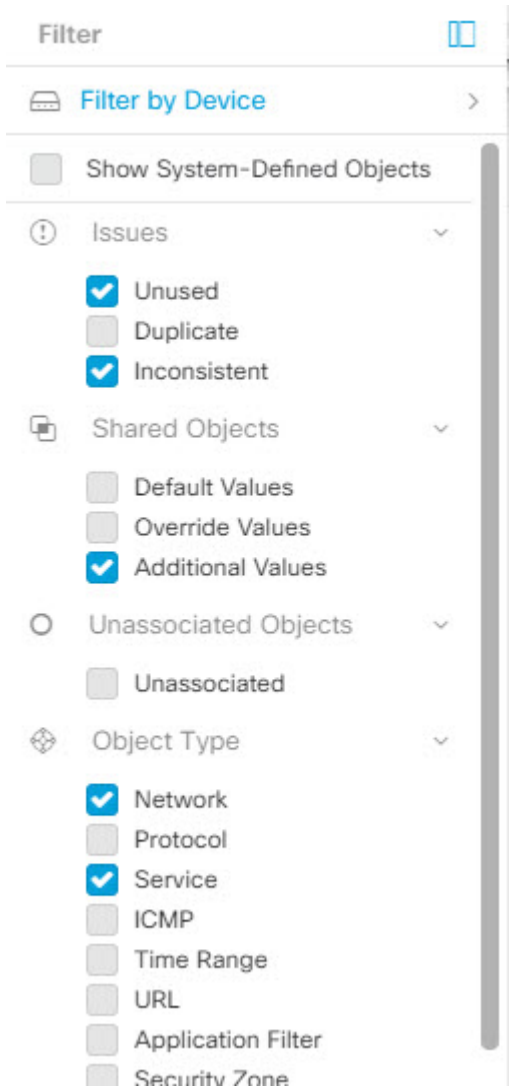
To filter, click in the left-hand pane of the Inventory, Policies, and Objects tabs:

The Inventory 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.

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 objects that are "Issues (Used OR Inconsistent) AND Shared Objects with Additional Values AND Objects of type Network OR Service.



Object Filters

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

- **All Objects** – This filter provides you all the objects available from all the devices you have on-boarded in CDO. This filter is useful to browse all your objects, or as a starting point to search or further apply sub-filters.
- **Shared Objects** – This quick filter shows you all the Objects that CDO has found to be shared on more than one device.
- **Objects By Device** – Lets you pick a specific device so that you can see objects found on the selected device.

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 Objects Filter

Some devices come with pre-defined 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 Objects is **off** by default. To display system objects in the object table, check **Show System 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.

Step 1 In the CDO navigation bar on the left, click **Objects** and choose an option.

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 CDO 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 CDO 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.

Step 1 In the CDO navigation bar on the left, 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 mulitple objects.

Delete a Single Object

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

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

Step 1 In the CDO navigation bar on the left, choose **Objects** and choose an option.

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 Preview and Deploy Configuration Changes for All Devices 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.

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 Preview and Deploy Configuration Changes for All Devices 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 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 CDO.

Table 1: Pemitted Values of Network Objects

Device type	IPv4 / IPv6	Single Address	Range of addresses	Fully Qualified Domain Name	Subnet using CIDR Notation
Meraki	IPv4	Yes	Yes	Yes	Yes

Table 2: Pemitted Contents of a Network Group

Device type	IP Value	Network Object	Network Groups
Meraki	Yes	Yes	Yes

Reusing Network Objects Across Products

If you have a Cisco Defense Orchestrator tenant with a cloud-delivered Firewall Management Center and one or more on-prem management centers onboarded to your tenant:

- When you create a Secure Firewall Threat Defense, FDM-managed threat defense, ASA, or Meraki network object or group, a copy of the object is also added to the objects list on the **Objects > Other FTD Objects** page used when configuring cloud-delivered Firewall Management Center, and vice versa.
- When you create a Secure Firewall Threat Defense, FDM-managed threat defense, or ASA network object or group, an entry is created in the **Devices with Pending Changes** page for each On-Prem Firewall Management Center for which **Discover & Manage Network Objects** is enabled. From this list, you can choose and deploy the object to the on-prem management center on which you want to use the object and discard the ones that you do not want. Navigate **Tools & Services** > **Firewall Management Center**, select the on-prem management center, and click **Objects** to see your objects in the On-Prem 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 threat defense, ASA, or Meraki network object will not be replicated on the **Objects > Other FTD Objects** page of Cisco Defense Orchestrator
- Network objects and groups in onboarded threat defense devices that are managed by on-premises Secure Firewall Management Center are not replicated on the **Objects > Other FTD Objects** page 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 CDO objects page if they are used in policies that were deployed to FTD devices.
- Sharing Network Objects between CDO 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 CDO and On-Prem Management Center is not automatically enabled on CDO for new on-prem management centers onboarded to CDO. If your network objects are not being shared with On-Prem Management Center, ensure **Discover & Manage Network Objects** toggle button is enabled for the on-prem management center in **Settings** or contact TAC to have the features enabled on your tenant.

Viewing Network Objects

Network objects you create using CDO and those CDO 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.

Objects Associated with Meraki Devices

About Objects Used with Meraki Devices

The Meraki dashboard utilizes groups of IP addresses, protocols, or port ranges in source and destination fields in outbound access control rules. Once onboarded, CDO translates IP address into network objects, and application layer protocol values into either service objects or protocol objects.

A single rule in CDO can translate into multiple rules in the dashboard. For example, if you add an ASA protocol group that includes both TCP and UDP protocols to a single access control rule in CDO, CDO translates the one CDO rule into multiple rules in the dashboard: one rule containing a TCP protocol and one rule containing a UDP protocol.

Note that the Meraki dashboard and CDO both support CIDR subnet notation. For more information on layer 3 switch interfaces and MX device layout, see the Meraki Knowledge Base.

Which Objects Can You Use With a Meraki Device in CDO?

There are no objects in Cisco Defense Orchestrator (CDO) that are exclusive to MX devices. Instead, you can create or share FTD, FDM, and ASA objects and associate these objects in rules that are deployed to the device. Because Meraki is not fully compatible with FTD and ASA objects, there may be a few limitations that affect how the MX device uses objects.

Note that if you associate an FTD, FDM, and ASA objects with a MX device, that object becomes shared. Any changes to that object will affect all the devices it is shared with and the devices' configuration status will appear as *Not Synced*. See Shared Objects for more information. For additional object states that could affect your objects, see the **Related Articles** section listed at the bottom of this page.

Meraki does not support objects containing IPv6 addresses or FQDNs.

Object in CDO	Compatible with Meraki
Protocol Objects	TCP, UDP, ICMP
Network Objects	yes
Network Groups	yes
Service Objects	yes
ASA Service Groups	no
FTD Service Groups	no

Local Network Objects and Object Groups From the Meraki Cloud

Network objects and object groups provide easier management of firewall rules for Meraki devices. They serve as labels to IP Subnets and FQDN that can be used on access policies such as firewall rules. If there are needs to modify multiple access policies that use the same IP Subnets or FQDN, you only need to modify the network object to have it reflect on all policies.At this time, you must use the Meraki dashboard to create and modify these objects. For more information about what these objects can do for your environment, see Meraki's Network Objects Highlights.

Note Once a device configuration referencing a Meraki network object or network object group is onboarded or synchronized to the CDO UI, these objects are displayed as **FTD Network** objects.

These objects and object groups are **read-only** in CDO.

What Do Meraki Rules Look Like in CDO

You can view the objects from the device's policy page, or you can filter the objects page based on device. From the policy page you can view, edit, and reorder the access control rules. Because CDO translates the outbound rules from the Meraki dashboard into access control rules with objects, rules and protocols from the Meraki dashboard may look different. The following table addresses the new names for protocols once the device is onboarded to CDO:

Rule or Protocol Header in the Meraki dashboard	Rule or Object Header in CDO
Policy	Action
Source IP	Network Object or Network Group
Destination IP	Network Object or Network Group
Source Port	Network Object or Network Group
Destination Port	Network Object or Network Group
Layer 3 Application Protocol	Ports (Protocol Groups, Port Groups, or Service Objects)

The following is an example of what the outbound rules from the Meraki dashboard look in CDO:

Create a Local Meraki Network Object

A local Meraki network object must be made in the Merkai dashboard. If you have a Meraki device that has not been onboarded to CDO yet, any pre-existing local objects are onboarded with the device; if you have a Meraki device that **has** been onboarded, sychronize the device in CDO to read the new configuration and local objects.

Note Once a device configuration referencing a Meraki network object or network object group is onboarded or synchronized with the CDO UI, these objects are displayed as **FTD Network** objects or object groups.

These objects and object groups are **read-only** in CDO.

Before you begin

If you have not enabled Merkai's **Open Beta Network Objects**, log into the Meraki dashboard and navigate to **Organization** > **Policy Object** to enroll and get access to local objects and object groups

Step 1 Log into the Meraki dashboard and create a local object or a local object group. See the Meraki Network Objects Configuration Guide for more information.

Step 2 Log into CDO.

Note: If you have not yet onboarded your Meraki device to CDO, see Onboard an MX Device to CDO for more information. Onboarding a device also onboards all the pre-existing objects.

Step 3 In the navigation pane, click **Inventory**.

Step 4 Locate the Merkai device and select it so the device row is highlighted. The device status is **Conflict detected**. In the pane located to the right, select either **Review Conflict** to review the changes made to the device's configuration or **Accept without Review** to accept all configuration changes.

Create or Edit a Meraki Network Object or Network Group

MX devices use the same format as Firepower and ASA **network objects** and can contain a host name, an IP address or a subnet address expressed in CIDR notation. **Network groups** are a collection of network objects and other individual addresses or subnets you add to the group. Network objects and network groups are used in access rules. You can create, read, update, and delete network objects and network groups using CDO.

IP addresses that can be added to network objects

Device type	IPv4 / IPv6	Single Address	Range of addresses	Fully Qualified Domain Name	Subnet using CIDR Notation
MX	IPv4	Yes	Yes	No	Yes

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

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

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

Changes you make to network objects and groups on the **Objects > FTD Network Objects** page are reflected in the corresponding cloud-delivered Firewall Management Center network object or group on the **Objects > Other FTD Objects** page. In addition, an entry is created in the **Devices with Pending Changes** page for each on-prem management center with **Discover & Manage Network Objects** enabled, from which you can choose and deploy the changes to the on-prem 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 a Meraki Network Object

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

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

Step 1 In the CDO navigation bar on the left, click **Objects > Meraki Objects**.

Step 2 Click  , then click **FTD** > **Network** or **ASA** > **Network**.

Step 3 Enter an object name.

Step 4 Select **Create a network object**.

Step 5 In the Value section, enter a single IP address or a subnet address expressed in CIDR notation.

Step 6 Click **Add**.

Step 7 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Create a Meraki Network Group

A network group is made up of multiple network objects or IP addresses.

If you want your network group to be made up of network objects, use the "Create a Network Object" procedure above to create individual network objects for your IP addresses.

Note If cloud-delivered Firewall Management Center is deployed on your tenant:

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

Step 1 In the CDO navigation bar on the left, click **Objects** > **Meraki Objects**.

Step 2 Click  , then click either **FTD** > **Network** or **ASA** > **Network**.

Step 3 Enter an object name.

Step 4 Select **Create a network group**.

Step 5 Click **Add Object**, select the network object from the list and click **Select**. Continue to do this until you have added all the network objects you want.

Step 6 Click **Add**.

Step 7 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Edit a Firepower Network Object or Network Group

Caution If cloud-delivered Firewall Management Center is deployed on your tenant:

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

Step 1 In the CDO navigation bar on the left, click **Objects** > **Meraki Objects**.

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

Step 3 Select the object you want to edit.

Step 4 Click the edit button  in the details pane.

Step 5 Edit the values in the dialog box in the same fashion that you created them in the procedures above.

Step 6 Click **Save**.

Step 7 CDO displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Related Information

- Objects Associated with Meraki Devices
- Create or Edit a Meraki Service Object
- Resolve Unused Object Issues
- Resolve Duplicate Object Issues

- Change Log

Deleting Network Objects and Groups in CDO

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

Deleting a network object or group from the **Objects > FTD Network Objects** page deletes the replicated network object or group from the **Objects > Other FTD Objects** page and vice-versa.

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. CDO 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. CDO recognizes these objects in ASA and Firepower configurations when those devices are onboarded and CDO gives them their own filter of "ICMP" so you can find the objects easily.

Using CDO, you can rename or remove ICMP objects from an ASA configuration. You can use CDO 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

Create or Edit a Meraki Service Object

About Service Objects

Service objects are reusable components that specify a TCP/IP protocol and a port. CDO categorizes these objects as service objects. When you deploy to the MX device, CDO translates the objects into protocols or port ranges. See Objects Associated with Meraki Devices for more information about how CDO handles Meraki protocols as objects.

Create a Service Object

Step 1 In the CDO navigation bar on the left, click **Objects > Meraki Objects**.

Step 2 Click  , then click **FTD** > **Service** or **ASA** > **Service**.

Step 3 Enter an object name and description.

Step 4 Select **Create a service object**.

Step 5 Click the **Service Type** button and select the protocol for which you want to create an object.

Step 6 Enter the information to identify the protocol by taking one of these actions:

- Enter the specific port number for the TCP or UDP port.
- Select the ICMP or ICMPv6 message type.
- If you selected the "other" service type, select one of the TCP/IP protocols from the list.

Step 7 Click **Add**.

Step 8 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Create a Service Group

Step 1 In the CDO navigation bar on the left, click **Objects** > **Meraki Objects**.

Step 2 Click  , then click **FTD** > **Service**.

Note Meraki does not support ASA service groups.

Step 3 Enter an object name and description.

Step 4 Select **Create a service group.**

Step 5 Add an existing object by clicking **Add Object,** selecting an object, and clicking **Select**. Repeat this step to add more objects.

Step 6 Click **Add** when you are done adding service objects and service values to the service group.

Step 7 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Edit a Service Object or a Service Group

Step 1 In the CDO navigation bar on the left, click **Objects** > **Meraki Objects**.

Step 2 Filter the objects to find the object you want to edit and then select the object in the object table.

Step 3 In the details pane, click edit  .

Step 4 Edit the values in the dialog box in the same fashion that you created them in the procedures above.

Step 5 Click **Save**.

Step 6 CDO displays the policies that will be affected by the change. Click **Confirm** to finalize the change to the object and any policy affected by it. The object is now ready to be used in the Meraki policy.

Step 7 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

Related Information

- Objects Associated with Meraki Devices
- Resolve Unused Object Issues
- Resolve Duplicate Object Issues
- Change Log

Manage Security Policies in CDO

Security policies examine network traffic with the ultimate goal of allowing the traffic to its intended destination or dropping it if a security threat is identified. You can use CDO to configure security policies on many different types of devices.

- Meraki Access Control Policy, on page 20

Meraki Access Control Policy

Meraki MX devices may have been managed by the Meraki dashboard before you onboard to CDO and the device may already have some outbound rules. These rules will appear as access control rules in CDO. You can modify these rules and create additional rules within the access control policy. To customize your access control policy, create and attach objects. See the related articles at the bottom for more information.

Note The action of the Meraki access control policy is **Allow** by default. You cannot change the action.

Use this procedure to edit a Meraki access control policy using CDO:

Step 1 Open the **Inventory** page.

Step 2 Click the **Templates** tab.

Step 3 Click the **Meraki** tab and select the Meraki MX device template whose access control policy you want to edit.

Step 4 In the **Management** pane at the right, select **Policy**.

Step 5 Do any of the following:

- To create a new rule, click the blue plus button .
- To edit an existing rule, select the rule and click the edit button in the Actions pane. (Simple edits may also be performed inline without entering edit mode.)
- To delete a rule you no longer need, select the rule and click the remove button in the Actions pane.
- To move a rule within the policy, select the rule in the access control table and click the up or down arrow at the end of the rule row to move the rule.

Step 6 In the **Order** field, select the position for the rule within the policy. Network traffic is evaluated against the list of rules in numerical order, 1 to "last."

Rules are applied on a first-match basis, so you must ensure that rules with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

The default is to add the rule to the end of the list. If you want to change a rule's location later, edit this option.

Step 7 Enter the rule name. You can use alphanumeric characters, spaces, and these special characters: + . _ -

Note: The **Name** of the access control rule is used as the name of the rule in CDO while the **Remark** field is treated as the name of the rule in the Meraki dashboard. The two fields are not dependent on each other.

Step 8 Select the action to apply if the network traffic is matched by the rule:

- **Block**-Drop the traffic unconditionally. The traffic is not inspected.
- **Allow**-Allow the traffic subject to the intrusion and other inspection settings in the policy.

Note You can only set or modify the rule action. You cannot change the default policy action from CDO.

Step 9 Define the traffic matching criteria by using any combination of attributes in the following tabs:

- **Source**-Click the **Source** tab and add or remove networks (which includes networks and continents) or ports from which the network traffic originated. The default value is "Any."
- **Destination**-Click the **Destination** tab and add or remove networks (which includes networks and continents), or ports on which the traffic arrives. The default value is "Any."

Note The source and destination networks must be within one of the configured VLAN subnets or, if a VLAN subnet is not manually configured, the default VPN subnet. Deploying a rule that includes an invalid source or destination network will fail.

Step 10 Click **Save**.

Step 11 Preview and Deploy Configuration Changes for All Devices now the changes you made, or wait and deploy multiple changes at once.

What to do next

Related Articles:

- Objects Associated with Meraki Devices
- Create or Edit a Meraki Service Object
- Create or Edit a Meraki Network Object or Network Group

Meraki Templates

The Meraki template is a network configuration that is shared by multiple sites/networks. Individual site networks can be bound to a template network, so changes to a single template will trickle down to all bound networks; in CDO, bound networks are displayed as bound devices. This is ideal if you want one policy across multiple networks in different locations. To configure more than one network to a single template, see Managing Multiple Networks with Configuration Templates. See Meraki Templates Best Practices for more information

on what a Meraki template is, how you can plan on using templates in your network, and how to setup your template network.

Meraki templates work in the same way as the Meraki devices do, where you must first configure the template through the Meraki dashboard prior to onboarding to CDO. When you onboard a template to CDO, any existing rules or groups of IPs are About Device Configuration Changes into CDO and translated into objects. Once synced, the Device Details pane on the **Inventory** page displays the template name as well as how many networks, displayed as bound devices, are associated with it. This means you can also manage and modify/deploy the policies that are associated with the template and the bound networks from CDO. See Onboard Meraki Templates to Defense Orchestrator for more information.

Related Information

- How Does CDO Communicate With Meraki
- Objects Associated with Meraki Devices
- About Device Configuration Changes

About Device Configuration Changes

In order to manage a device, CDO must have its own copy of the device's configuration stored in its local database. When CDO "reads" a configuration from a device it manages, it takes a copy of the device's configuration and saves it. The first time CDO reads and saves a copy of a device's configuration is when the device is onboarded. These choices describe reading a configuration for different purposes:

- **Discard Changes**: This action is available when a device's configuration status is "Not Synced." In the Not Synced state, there are changes to the device's configuration pending on CDO. This option allows you to undo all pending changes. The pending changes are deleted and CDO overwrites its copy of the configuration with copy of the configuration stored on the device.
- **Check for Changes**: This action is available if the device's configuration status is Synced. Clicking Checking for Changes directs CDO to compare its copy of the device's configuration with the copy of the configuration stored on the device. If there is a difference, CDO immediately overwrites its copy of the device's configuration with the copy stored on the device.
- **Review Conflict** and **Accept Without Review**: If you have enabled Conflict Detection on a device, CDO checks for configuration changes made on the device every 10 minutes. If the copy of the configuration stored on the device has changed, CDO notifies you by displaying the "Conflict Detected" configuration status.
  - **Review Conflict**: Click Review Conflict allows you to review changes made directly on a device and accept or reject them.
  - **Accept Without Review**: This action overwrites CDO's copy of a device's configuration with the latest copy of the configuration stored on the device. CDO does not prompt you to confirm the differences in the two copies of the configuration before taking the overwriting action.

Read All: This is a bulk operation. You can select more than one device, in any state, and click **Read All** to overwrite all the devices' configurations stored on CDO with the configurations stored on the devices.

- **Deploy Changes**: As you make changes to a device's configuration, CDO saves the changes you make to its own copy of the configuration. Those changes are "pending" on CDO until they are deployed to

the device. When there are changes to a device's configuration that have not been deployed to the device, the device is in the Not Synced configuration state.

Pending configuration changes have no effect on the network traffic running through the device. Only after CDO deploys the changes to the device do they have an effect. When CDO deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. It does not overwrite the entire configuration file stored on the device. Deployments can be initiated for a single device or on more than one device simultaneously.

- **Discard All** is an option that is only available after you click **Preview and Deploy...**. After clicking Preview and Deploy, CDO shows you a preview of the pending changes in CDO. Clicking **Discard All** deletes all pending changes from CDO and does not deploy anything to the selected device(s). Unlike "Discard Changes" above, deleting the pending changes is the end of the operation.

Read All Device Configurations

If a configuration change is made to a device outside of Cisco Defense Orchestrator (CDO), the device's configuration stored on CDO and the device's local copy of its configuration are no longer the same. You many want to overwrite CDO's copy of the device's configuration with the configuration stored on the device to make the configurations the same again. You can perform this task on many devices simultaneously using the **Read All** link.

See About Device Configuration Changes for more information about how CDO manages the two copies of the device's configuration.

Here are three configuration statuses where clicking **Read All** will overwrite CDO's copy of the device's configuration with the device's copy of the configuration.

- **Conflict Detected**-If conflict detection is enabled, CDO polls the devices it manages every 10 minutes for changes made to their configurations. If CDO finds that the configuration on the device has changed, CDO displays a "Conflict detected" configuration status for the device.
- **Synced**-If the device is in a synced state, and you click **Read All**, CDO immediately checks the devices to determine if there have been any changes made to its configurations directly. After clicking **Read All**, CDO confirms your intent to overwrite its copy of the device's configuration and then CDO performs the overwrite.
- **Not Synced**-If the device is in the Not Synced state, and you click **Read All**, CDO warns you that there are pending changes made to to the device's configuration using CDO and that proceeding with the Read All operation will delete those changes and then overwrite CDO's copy of the configuration with the configuration on the device. This Read All functions like Discard Configuration Changes.

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 (Optional) Create a change request label to identify the results of this bulk action easily in the Change Log.

Step 5 Select the devices whose configurations you want to save CDO. Notice that CDO only provides command buttons for actions that can be applied to all the selected devices.

Step 6 Click **Read All**.

Step 7 CDO warns you if there are configuration changes staged on CDO, for any of the devices you selected, and asks if you want to continue with the bulk reading configurations action. Click **Read All** to continue.

Step 8 Look at the notifications tab for the progress of the Read All configurations operation. If you want more information about how individual actions in the bulk operation succeeded or failed, click the blue Review link and you will be directed to the Jobs page.

Step 9 If you created and activated a change request label, remember to clear it so that you don't inadvertently associate other configuration changes with this event.

Related Information

- About Device Configuration Changes
- Discard Configuration Changes
- Check for Configuration Changes

Preview and Deploy Configuration Changes for All Devices

CDO informs you when you have made a configuration change to a device on your tenant, but you have not deployed that change, by displaying an orange dot on the Deploy icon

. The devices affected by these changes show the status "Not Synced" in the Devices and **Services** page. By clicking **Deploy**, you can review which devices have pending changes and deploy the changes to those devices.

Note For every new FDM or FTD network object or group that you create and make changes to, CDO creates an entry in this page for all on-prem management centers that are managed by CDO.

This deployment method is available for all supported devices.

You can use this deployment method for single configuration changes or wait and deploy multiple changes at once.

Step 1 In the top right corner of the screen, click the **Deploy** icon .

Step 2 Select the devices with changes you want to deploy. If a device has a yellow caution triangle, you can not deploy changes to that device. Hover your mouse over the yellow caution triangle to find out why you can't deploy changes to that device.

Step 3 (Optional) If you want to see more information about a pending change, click the **View Detailed Changelog** link to open the change log associated with that change. Click the **Deploy** icon to return to the **Devices with Pending Changes** page.

Step 4 (Optional) Create a change request to track your changes without leaving the **Devices with Pending Changes** page.

Step 5 Click **Deploy Now** to deploy the changes immediately to the devices you selected. You'll see the progress in the Active jobs indicator in the Jobs tray.

Step 6 (Optional) After the deployment has finished, click **Jobs** in the CDO navigation bar. You will see a recent "Deploy Changes" job showing the results of the deployment.

Step 7 If you created a change request label, and you have no more configuration changes to associate with it, clear it.

What to do next

- About Scheduled Automatic Deployments

Deploy Changes to a device

Step 1 After you make a configuration change for a device using CDO and save it, that change is saved in CDO instance of the device's configuration.

Step 2 In the navigation bar, click **Inventory**.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab. You should see that the configuration status of the device you made changes to is now "Not synced."

Step 5 Deploy the changes using one of these methods:

- Select the device and in the Not Synced pane on the right, click **Preview and Deploy.** On the Pending Changes screen, review the changes. If you are satisfied with the pending version, click **Deploy Now**. After the changes are deployed successfully, you can view the change log to confirm what just happened.
- Click the **Deploy** icon  at the top-right of the screen. See Preview and Deploy Configuration Changes for All Devices, on page 24 for more information.

Cancelling Changes

If, when deploying a change from CDO to a device, you click **Cancel**, the changes you made are not deployed to the device. The process is canceled. The changes you made are still pending on CDO and can be edited further before you finally deploy them to FDM-managed device.

Discarding Changes

If, when previewing changes, you click **Discard all**, the changes you made, and any other changes any other user made but did not deploy to the device, are deleted. CDO reverts its pending configuration to the last read or deployed configuration before any changes were made.

Bulk Deploy Device Configurations

If you have made changes to multiple devices, for instance by editing a shared object, you can apply those change to all of the affected devices at once:

Step 1 In the navigation pane, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select all of the devices for which you have made configuration changes on CDO. These devices should show "Not Synced" status.

Step 5 Deploy the changes using one of these methods:

- Click the button at the top-right of the screen to view the **Devices with Pending Changes** window. This gives you a chance to review the pending changes on the devices you selected before you deploy them. Click **Deploy Now** to deploy the changes.

  Note If you see a yellow warning triangle next to a device on the **Devices with Pending Changes** screen, you cannot deploy a change to that device. Hover your mouse over the warning triangle for information about why changes cannot be deployed to that device.

- Click **Deploy All** on the details pane. Review any warnings and click **OK**. The bulk deployment starts immediately without a review of the changes.

Step 6 (Optional) Click the Jobs icon in the navigation bar to view the results of the bulk deploy.

About Scheduled Automatic Deployments

Using CDO, you can make configuration changes to one or more of the devices it manages and then schedule the changes to be deployed to those devices at a time that is convenient for you.

You can only schedule deployments if you Enable the Option to Schedule Automatic Deployments in the **Tenant Settings** tab of the Settings page. Once this option is enabled, you can create, edit, or delete scheduled deployments. A scheduled deployment deploys all the staged changes saved on CDO at the date and time set. You can also view and delete scheduled deployments from the Jobs page.

If there were changes made directly to the device that have not been About Device Configuration Changes to CDO, the scheduled deployment will be skipped until that conflict is resolved. The Jobs page will list any instance where a scheduled deployment fails. If **Enable the Option to Schedule Automatic Deployments** is turned off, all scheduled deployments are deleted.

Caution If you schedule a new deployment for multiple devices, and some of those devices already have deployments scheduled, the new scheduled deployment overwrites the existing scheduled deployments.

Note When you create a scheduled deployment, the schedule is created in your local time, not in the time zone of the device. Scheduled deployments *do not* automatically adjust for daylight savings time.

Schedule an Automatic Deployment

The deployment schedule can be a single event or a recurring event. You may find recurring automatic deployments a convenient way to line up recurring deployments with your maintenance window. Follow this procedure to schedule a one-time or a recurring deployment for a single device:

Note If you schedule a deployment for a device that has an existing deployment scheduled, the new scheduled deployment overwrites the existing deployment.

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select one ore more devices.

Step 5 In the Device Details pane, locate the Scheduled Deployments tab and click **Schedule**.

Step 6 Select when the deployment should occur.

- For a one-time deployment, click the **Once on** option to select a date and time from the calendar.
- For a recurring deployment, click the **Every** option. You can choose either a daily or once a week deployment. Select the **Day** and **Time** the deployment should occur.

Step 7 Click **Save**.

Edit a Scheduled Deployment

Follow this procedure to edit a scheduled deployment:

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select one or more devices.

Step 5 In the **Device Details** pane, locate the Scheduled Deployments tab and click **Edit** .

Step 6 Edit the recurrence, date, or time of a scheduled deployment.

Step 7 Click **Save**.

Delete a Scheduled Deployment

Follow this procedure to delete a scheduled deployment:

Note If you schedule a deployment for multiple devices, and then change or delete the schedule for some of the devices, the original scheduled deployment for the remaining devices will be preserved.

Step 1 In the navigation bar, click**Inventory**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select one or more devices.
Step 5 In the **Device Details** pane, locate the Scheduled Deployments tab and click **Delete** .

What to do next

- About Device Configuration Changes
- Read All Device Configurations, on page 23
- Preview and Deploy Configuration Changes for All Devices, on page 24

Check for Configuration Changes

Check for Changes to determine if the device's configuration has been changed directly on the device and it is no longer the same as the copy of the configuration stored on CDO. You will see the this option when the device is in the "Synced" state.

To check changes:

Step 1 In the navigation bar, click **Inventory**.
Step 2 Click the **Devices** tab.
Step 3 Click the appropriate device type tab.
Step 4 Select the device, whose configuration you suspect may have been changed directly on the device.
Step 5 Click **Check for Changes** in the Synced pane on the right.
Step 6 The behavior that follows is slightly different depending on the device:

- For Meraki device if there has been a change to the device's configuration, you will receive the message:

```
Reading the policy from the device. If there are active deployments on the device, reading will
start after they are finished.
```

  - Click **OK** to continue. The configuration on the device will overwrite the stored configuration on CDO.
  - Click **Cancel** to cancel the action.

- For device:

a. Compare the two configurations presented to you. Click **Continue**. The configuration labeled **Last Known Device Configuration** is the configuration stored on CDO. The configuration labeled **Found on Device** is the configuration saved on the ASA.

b. Select either:

1. **Reject** the out-of-band changes to keep the "Last Known Device Configuration."
2. **Accept** the out-of-band changes to overwrite the device's configuration stored in CDO with the configuration found on the device.

c. Click **Continue**.

Discard Configuration Changes

Click **Discard Changes** when you want to "undo" all the *undeployed* configuration changes you made to a device's configuration using CDO. When you click **Discard Changes**, CDO *completely overwrites* its local copy of a device's configuration with the configuration stored on the device.

When you click **Discard Changes**, your device's configuration status is in a **Not Synced** state. After you discard your changes, the copy of the configuration on CDO will be the same as the copy of the configuration on the device and the configuration status in CDO will return to Synced.

To discard, or "undo," all of your undeployed configuration changes for a device:

Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the device you have been making configuration changes to.

Step 5 Click **Discard Changes** in the **Not Synced** pane on the right.

- For FDM-managed devices-CDO warns you that "Pending changes on CDO will be discarded and the CDO configuration for this device will be replaced with the configuration currently running on the device." Click **Continue** to discard your changes.
- For Meraki devices-CDO deletes the change immediately.
- For AWS devices-CDO displays what you are about to delete. Click **Accept** or **Cancel**.

Out-of-Band Changes on Devices

Out-of-band changes refer to changes made directly on the device without using CDO. These changes may be made using the device's command-line interface over an SSH connection or by using a local manager like

the Adaptive Security Device Manager (ASDM) for the ASA, the FDM for the FDM-managed device, or for an On-Prem Firewall Management Center on the On-Prem Firewall Management Center user interface. An out-of-band change causes a conflict between the device's configuration stored on CDO and the configuration stored on the device itself.

Detecting Out-of-Band Changes on Devices

If Conflict Detection is enabled for an ASA, or an FDM-managed device, a Cisco IOS device, or an On-Prem Firewall Management Center, CDO checks the device every 10 minutes searching for any new changes made directly to the device's configuration outside of CDO.

If CDO finds that there are changes to the device's configuration that are not stored on CDO, it changes the **Configuration Status** of that device to the "Conflict Detected" state.

When Defense Orchestrator detects a conflict, one of two conditions is likely:

- There have been configuration changes made to the device directly that have not been saved to CDO's database.
- In the case of an FDM-managed device, there may be "pending" configuration changes on the FDM-managed device that have not been deployed.
- In the case of an On-Prem Firewall Management Center, there may be changes made, for instance, to objects outside CDO, which are pending to be synchronized with CDO or changes made in CDO which are pending to be deployed to the On-Prem Firewall Management Center.

Synchronizing Configurations Between Defense Orchestrator and Device

About Configuration Conflicts

On the **Inventory** page, you may see devices or services have the status "Synced," "Not Synced," or "Conflict Detected." To know the status of an On-Prem Firewall Management Center that you manage using CDO, navigate **Tools & Services** > **Firewall Management Center**.

- When a device is **Synced**, the configuration on Cisco Defense Orchestrator (CDO) and the configuration stored locally on the device are the same.
- When a device is **Not Synced**, the configuration stored in CDO was changed and it is now different that the configuration stored locally on the device. Deploying your changes from CDO to the device changes the configuration on the device to match CDO's version.
- Changes made to devices outside of CDO are called **out-of-band changes**. When out-of-band changes are made, you'll see the device state change to "Conflict Detected," if conflict detection is enabled for the device. Accepting the out-of-band changes, changes the configuration on CDO to match the configuration on the device.

Conflict Detection

When conflict detection is enabled, Cisco Defense Orchestrator (CDO) polls the device for the default interval to to determine if a change has been made to the device's configuration outside of CDO. If CDO detects that a change was made, it changes the configuration status for the device to **Conflict Detected**. Changes made to a device outside of CDO are called "out-of-band" changes.

In the case of an On-Prem Firewall Management Center that is managed by CDO, if there are changes that are staged and the device is in **Not Synced** state, CDO stops polling the device to check for changes. When there are changes made outside CDO which are pending to be synchronized with CDO and changes made in CDO which are pending to be deployed to the on-prem management center, CDO declares the on-prem management center to be in the **Conflict Detected** state.

Once this option is enabled, you can configure how often conflicts or OOB changes are detected per device. See Schedule Polling for Device Changes, on page 34 for more information.

Enable Conflict Detection

Enabling conflict detection alerts you to instances where changes have been made to a device outside of Defense Orchestrator.

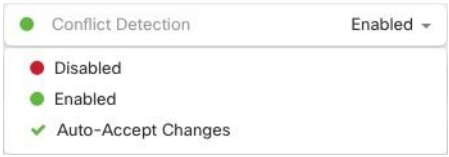
Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab.

Step 3 Select the appropriate device type tab.

Step 4 Select the device or devices for which you want to enable conflict detection.

Step 5 In the **Conflict Detection** box at the right of the device table, select **Enabled** from the list.



Automatically Accept Out-of-Band Changes from your Device

You can configure Cisco Defense Orchestrator (CDO) to automatically accept any change made directly to a managed device by enabling auto-accept changes. Changes made directly to a device without using CDO are referred to as out-of-band changes. An out-of-band change creates a *conflict* between the device's configuration stored on CDO and the configuration stored on the device itself.

The auto-accept changes feature is an enhancement to conflict detection. If you have auto-accept changes enabled on your device, CDO checks for changes every 10 minutes to determine if there have been any out-of-band changes made to the device's configuration. If there have been configuration changes, CDO automatically updates its local version of the device's configuration without prompting you.

CDO will ***not*** automatically accept a configuration change if there are configuration changes made on CDO that have not yet been deployed to the device. Follow the prompts on the screen to determine your next action.

To use auto-accept changes, you first enable the tenant to display the auto-accept option in the Conflict Detection menu on the **Inventory** page; then, you enable auto-accept changes for individual devices.

If you want CDO to detect out-of-band changes but give you the option to accept or reject them manually, enable Conflict Detection, on page 31 instead.

Configure Auto-Accept Changes

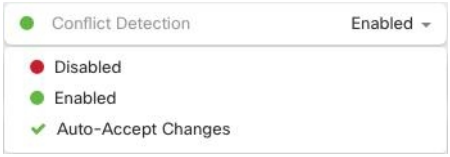
Step 1 Log in to CDO using an account with Admin or Super Admin privileges.

Step 2 From the CDO menu, navigate to **Settings** > **General Settings**

Step 3 In the **Tenant Settings** area, click the toggle to "**Enable the option to auto-accept device changes**." This enables the Auto-Accept Changes menu option to appear in the Conflict Detection menu on the **Inventory** page.

Step 4 Open the **Inventory** page and select the device for which you want to automatically accept out-of-band changes.

Step 5 In the **Conflict Detection** menu, select **Auto-Accept Changes** in the drop-down menu.



Disabling Auto-Accept Changes for All Devices on the Tenant

Step 1 Log-in to CDO using an account with Admin or Super Admin privileges.

Step 2 From the CDO menu, navigate **Settings** > **General Settings**

Step 3 In the **Tenant Settings** area, disable the "**Enable the option to auto-accept device changes**" by sliding the toggle to the left so it shows a grey X. This disables Auto-Accept Changes option in the Conflict Detection menu and disables the feature for every device on your tenant.

Note Disabling "Auto-Accept" will require you to review each device conflict before you can accept it into CDO. This includes devices previously configured to auto-accept changes.

Resolve Configuration Conflicts

This section provides information about resolving configuration conflicts that occur on the device.

Resolve the Not Synced Status

Use the following procedure to resolve a device with a "Not Synced" Configuration Status:

Step 1 In the navigation bar, click **Inventory**.

Note For an On-Prem Firewall Management Center, navigate **Tools & Services** > **Firewall Management Center** and select the FMC that is in **Not Synced** state and continue from Step 5.

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 reported as Not Synced.

Step 5 In the **Not synced** panel to the right, select either of the following:

- **Preview and Deploy...** -If you want to push the configuration change from CDO to the device, Preview and Deploy Configuration Changes for All Devices the changes you made now, or wait and deploy multiple changes at once.
- **Discard Changes** -If you do **not** want to push the configuration change from CDO to the device, or you want to "undo" the configuration changes you started making on CDO. This option overwrites the configuration stored in CDO with the running configuration stored on the device.

Resolve the Conflict Detected Status

CDO allows you to enable or disable conflict detection on each live device. If Conflict Detection, on page 31 is enabled and there was a change made to the device's configuration without using CDO, the device's configuration status will show **Conflict Detected**.

To resolve a "Conflict Detected" status, follow this procedure:

Step 1 In the navigation bar, click **Inventory**.

Note For an On-Prem Firewall Management Center, navigate **Tools & Services** > **Firewall Management Center** and select the FMC that is in **Conflict Detected** state and continue from Step 4.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device reporting the conflict and click **Review Conflict** in the details pane on the right.

Step 5 In the **Device Sync** page, compare the two configurations by reviewing the highlighted differences.

- The panel labeled "Last Known Device Configuration" is the device configuration stored on CDO.
- The panel labeled "Found on Device" is the configuration stored in the running configuration on the ASA.

Step 6 Resolve the conflict by selecting one of the following:

- **Accept Device changes**: This will overwrite the configuration **and any pending changes stored on CDO** with the device's running configuration.

Note As CDO does not support deploying changes to the Cisco IOS devices outside of the command line interface, your only choice for a Cisco IOS device will be to select **Accept Without Review** when resolving the conflict.

- **Reject Device Changes**: This will overwrite the configuration stored on the device with the configuration stored on CDO.

Note All configuration changes, rejected or accepted, are recorded in the change log.

Schedule Polling for Device Changes

If you have Conflict Detection, on page 31 enabled, or if you **Enable the option to auto-accept device changes** from the Settings page, CDO polls the device for the default interval to determine if a change has been made to the device's configuration outside of CDO. You can customize how often CDO polls for changes per device. These changes can be applied to more than one device.

If there is no selection configured for a device, the interval is automatically configured for "tenant default".

Note Customizing the interval per device from the **Inventory** page overrides the polling interval selected as the Default Conflict Detection Interval from the **General Settings** page.

After you enable **Conflict Detection** from the **Inventory** page or **Enable the option to auto-accept device changes** from the Settings page, use the following procedure to schedule how often you want CDO to poll your devices:

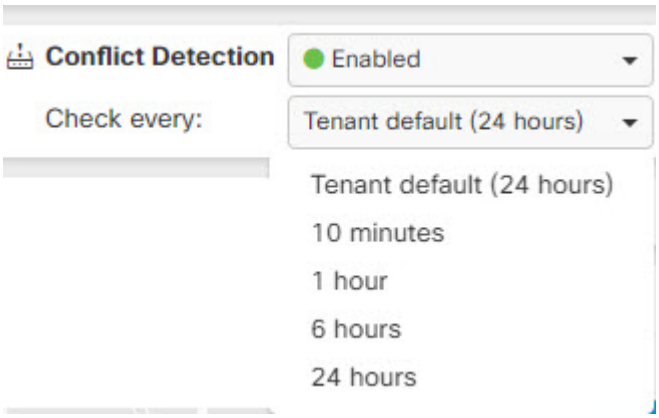
Step 1 In the navigation bar, click **Inventory**.

Step 2 Click the **Devices** tab to locate your device.

Step 3 Click the appropriate device type tab.

Step 4 Select the device or devices for which you want to enable conflict detection.

Step 5 In the same area as **Conflict Detection**, click the drop-down menu for **Check every** and select the desired polling interval:


Conflict Detection
Enabled
Check every:
Tenant default (24 hours)
Tenant default (24 hours)
10 minutes
1 hour
6 hours
24 hours