# Configuring On-Prem Firewall Management Center Devices

This chapter covers the following sections:



# Discover and Manage On-Prem Firewall Management Center Network Objects

If you have an On-Prem Firewall Management Center that you manage using CDO and you want to share and manage its objects, do the following:

**Step 1** From the CDO menu, navigate **Tools & Services** > **Firewall Management Center** to view the **Services** page.

**Step 2** If you already have onboarded an on-prem management center to CDO, select it.

If you want to onboard a new on-prem management center, see Onboard an On-Prem Firewall Management Center.

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

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

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

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

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

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

**Note** If you want to assign already-existing objects in CDO to your on-prem management center, choose the on-prem management center and click **Assign Objects** from the **Actions** pane.

**Related Information**

- Network Objects
- Preview and Deploy On-Prem Firewall Management Center Configurations
- Enable Conflict Detection for an On-Prem Firewall Management Center, on page 9

# 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.

**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

# 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

- Preview and Deploy On-Prem Firewall Management Center Configurations, on page 6
- Discard On-Prem Firewall Management Center Configuration Changes, on page 7

# 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.

# Preview and Deploy On-Prem Firewall Management Center Configurations

If you have made configuration changes to an object, for instance, changing a value or adding an override to an object, you can deploy all of those changes at once to your on-prem management center:

**Note** Note that this task only pushes the configuration changes to the on-prem management center. Ensure you manually deploy these changes to your threat defense devices on your on-prem management center. See Configuration Deployment in the *Cisco Secure Firewall Management Center Device Configuration Guide* for more information.

**Step 1** In the navigation pane, click **Tools & Services** > **Firewall Management Center** and select the On-Prem Firewall Management Center, to which you want to preview and deploy changes.

**Note** CDO detects that your on-prem management center is out of sync and displays the status as **Not Synced**.

**Step 2** Click **Preview and Deploy** on the details pane on the right.

**Step 3** Review any warnings and click **Deploy Now**. The deployment starts immediately without a review of the changes. Click **Discard All** if you do not want to proceed with the deploy after previewing.

**Step 4** Alternatively, you can also click the button at the top-right of the screen to view the **Devices with Pending Changes** window. Select the devices you want and review the pending changes on the devices that you selected before you deploy them.

**Step 5** Click **Deploy Now** to deploy the changes.

# 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**.

# Discard On-Prem Firewall Management Center Configuration Changes

If you want to undo all the configuration changes you made in CDO, for instance to the objects that are shared between your CDO and on-prem management center, use this procedure. Note that when you do this, CDO *completely overwrites* its local copy of the configuration with the configuration stored on the device.

**Step 1** In the navigation pane, click **Tools & Services** > **Firewall Management Center**.

**Step 2** Select the On-Prem Firewall Management Center, for which you want to discard changes.

**Step 3** Click **Discard Changes** in the **Not Synced** pane on the right.

When you click **Discard Changes**, your on-prem management center'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 on-prem management center and the configuration status in CDO returns to **Synced**.

# 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 12 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.

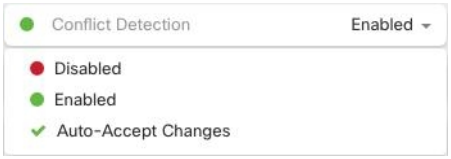
**Step 1** In the navigation bar, click **Inventory**.

**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.




# Enable Conflict Detection for an On-Prem Firewall Management Center

Enabling conflict detection for an On-Prem Firewall Management Center keeps you informed 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.

**Step 1** In the navigation bar, click **Tools & Services** > **Firewall Management Center**.

**Step 2** From the list, select the on-prem management center for which you want to enable conflict detection.

**Step 3** In the **Conflict Detection** box on the right pane, select **Enabled** from the list.

**Note** Unlike other devices managed by CDO, for an on-prem management center, you can either enable or disable conflict detection; you cannot opt to auto-accept changes.

# 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. For on-prem management center, you can do this from the **Services** page by navigating **Tools & Services** > **Firewall Management Center** and selecting the FMC.

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 8 instead.

# Configure Auto-Accept Changes

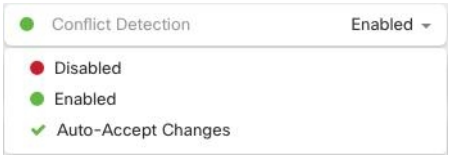
**Step 1** Log in to CDO using an account with Admin or Super Admin privileges.

**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 8 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 8 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:

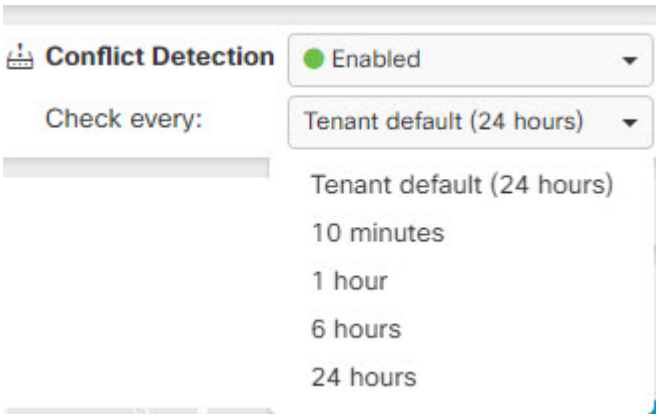
**Step 1** In the navigation bar, click **Inventory**.

**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