Configuring On-Premises Firewall Management Center Devices

This chapter covers the following sections:

View Onboarded On-Premises Management Center

To view onboarded on-premises management centers follow these steps:

1. In the left pane, click **Administration** > **Integrations** > **Firewall Management Center**.
2. Click the **FMC** tab.

View On-Premises Management Center High Availability Pair

The high availability pair is displayed in the **Services** page. On expanding the pair, you can see the primary and secondary on-premises management center nodes along with their current statuses.

To cross-launch the active on-premises management center, perform these steps:

1. In the **Services** page, check the corresponding high availability pair.
2. In the right pane, click the functionality you want to open in the on-premises management center.

   The **Verify FMC Cross Launch URL** window is displayed. By default, the public IP address or FQDN of the currently active on-premises management center is shown and will be used to open the on-premises management center. If needed, you can specify the URL of the standby on-premises management center to cross-launch it.

You can add cross-launch URLs to each on-premises management center node. When cross-launching from the pair, the active node is cross-launched and you need not verify which node is currently active.

To cross-launch to a specific on-premises management center node, perform these steps:

1. Expand the high availability pair and click primary or secondary on-premises management center node you want to launch.

2. In the **External Links** pane on the right, click **FMC Cross Launch URL** to cross-launch the selected on-premises management center.

   To update the public IP address or the FQDN and the port number of your on-premises management centerhover over the **FMC Cross Launch URL** and click the edit icon.

Note If you either break high availability or switch roles on the on-premises management center (version 7.4.x or earlier), you must disable the SecureX integration and then enable it again on the secondary on-premises management center. To do this, navigate to the secondary on-premises management center, choose .

Breaking a high-availability on-premises management center pair converts the participating management centers into two standalone on-premises management centers.

Discover and Manage On-Prem Firewall Management Center Network Objects

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

Procedure

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

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

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

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

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

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

Note

- You cannot turn the **Discover & Manage Network Objects** toggle on if the on-premises management center that you have selected has one or more child domains or has the 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-premises management center onboarded to Security Cloud Control, this toggle button needs to be enabled manually. Once you enable this option, Security Cloud Control starts to discover objects from your on-premises management center, which you can share, manage, and use to set consistent object definitions across other platforms managed by Security Cloud Control.

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

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

Related Information

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

Reading, Discarding, and Deploying Configuration Changes

Read All Device Configurations

If a configuration change is made to a device outside of Security Cloud Control, the device's configuration stored on Security Cloud Control and the device's local copy of its configuration are no longer the same. You many want to overwrite Security Cloud Control'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 Reading, Discarding, Checking for, and Deploying Configuration Changes for more information about how Security Cloud Control manages the two copies of the device's configuration.

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

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

Procedure

Step 1 In the left pane, click **Security Devices**.

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 Security Cloud Control. Notice that Security Cloud Control only provides command buttons for actions that can be applied to all the selected devices.

Step 6 Click **Read All**.

Step 7 Security Cloud Control warns you if there are configuration changes staged on Security Cloud Control, 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

- Reading, Discarding, Checking for, and Deploying Configuration Changes
- Discard Changes

Preview and Deploy Configuration Changes for All Devices

Security Cloud Control informs you when you have made a configuration change to a device in 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 **Security Devices** page. By clicking **Deploy**, you can review which devices have pending changes and deploy the changes to those devices.

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.

Procedure

Step 1 In the menu bar of Security Cloud Control click the **Deploy** button .

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

Step 6 If you created a change request label, and you have no more configuration changes to associate with it, clear it.

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:

Procedure

Step 1 In the left pane, click **Security Devices**.

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 Security Cloud Control. 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-Premises 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-premises management center:

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

Procedure

Step 1 In the navigation pane, click **Administration** > **Integrations** > **Firewall Management Center** and select the On-Premises Firewall Management Center, to which you want to preview and deploy changes.

Note
Security Cloud Control detects that your on-premises 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 Security Cloud Control. When you click **Discard Changes**, Security Cloud Control *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 Security Cloud Control will be the same as the copy of the configuration on the device and the configuration status in Security Cloud Control will return to Synced.

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

Procedure

Step 1 In the left pane, click **Security Devices**.

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-Security Cloud Control warns you that "Pending changes on Security Cloud Control will be discarded and the Security Cloud Control configuration for this device will be replaced with the configuration currently running on the device." Click **Continue** to discard your changes.
- For Meraki devices-Security Cloud Control deletes the change immediately.

- For AWS devices-Security Cloud Control displays what you are about to delete. Click **Accept** or **Cancel**.

Discard On-Premises Firewall Management Center Configuration Changes

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

Procedure

Step 1 In the left pane, click **Administration** > **Integrations** > **Firewall Management Center**.

Step 2 Select the On-Premises 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-premises management center's configuration status is in a **Not Synced** state. After you discard your changes, the copy of the configuration on Security Cloud Control will be the same as the copy of the configuration on the on-premises management center and the configuration status in Security Cloud Control returns to **Synced**.

Out-of-Band Changes on Devices

Out-of-band changes refer to changes made directly on the device without using Security Cloud Control. 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-Premises Firewall Management Center on the On-Premises Firewall Management Center user interface. An out-of-band change causes a conflict between the device's configuration stored on Security Cloud Control 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-Premises Firewall Management Center, Security Cloud Control checks the device every 10 minutes searching for any new changes made directly to the device's configuration outside of Security Cloud Control.

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

When Security Cloud Control 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 Security Cloud Control'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-Premises Firewall Management Center, there may be changes made, for instance, to objects outside Security Cloud Control, which are pending to be synchronized with Security Cloud Control or changes made in Security Cloud Control which are pending to be deployed to the On-Premises Firewall Management Center.

Synchronizing Configurations Between Security Cloud Control and Device

About Configuration Conflicts

In the **Security Devices** page, you may see devices or services have the status "Synced," "Not Synced," or "Conflict Detected." To know the status of an On-Premises Firewall Management Center that you manage using Security Cloud Control, navigate **Administration** > **Integrations** > **Firewall Management Center**.

- When a device is **Synced**, the configuration on Security Cloud Control) and the configuration stored locally on the device are the same.

- When a device is **Not Synced**, the configuration stored in Security Cloud Control was changed and it is now different that the configuration stored locally on the device. Deploying your changes from Security Cloud Control to the device changes the configuration on the device to match Security Cloud Control's version.

- Changes made to devices outside of Security Cloud Control 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 Security Cloud Control to match the configuration on the device.

Conflict Detection

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

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

Procedure

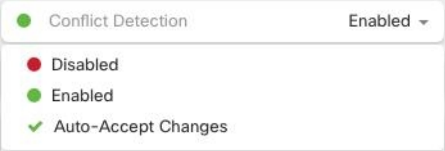
Step 1 In the left pane, click **Security Devices**.

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.



● Conflict Detection Enabled

Enable Conflict Detection for an On-Premises Management Center

Enabling conflict detection for an on-premises management center keeps you informed when there are changes made outside Security Cloud Control which are pending to be synchronized with Security Cloud Control and changes made in Security Cloud Control which are pending to be deployed to the on-prem management center.

Procedure

Step 1 In the navigation bar, click **Administration** > **Integrations** > **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 Security Cloud Control, for an on-premises 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 Security Cloud Control to automatically accept any change made directly to a managed device by enabling auto-accept changes. Changes made directly to a device without using Security Cloud Control are referred to as out-of-band changes. An out-of-band change creates a *conflict* between the device's configuration stored on Security Cloud Control 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, Security Cloud Control 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, Security Cloud Control automatically updates its local version of the device's configuration without prompting you.

Security Cloud Control will ***not*** automatically accept a configuration change if there are configuration changes made on Security Cloud Control 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 **Security Devices** page; then, you enable auto-accept changes for individual devices. For on-premises management center, you can do this from the **Services** page by navigating **Administration** > **Integrations** > **Firewall Management Center** and selecting the FMC.

If you want Security Cloud Control 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

Procedure

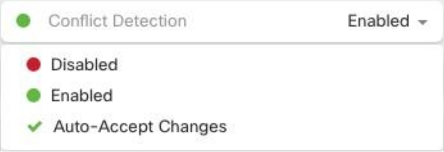
Step 1 Log in to Security Cloud Control using an account with Admin or Super Admin privileges.

Step 2 In the left pane, click **Administration** > **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 **Security Devices** page.

Step 4 In the left pane, click **Security Devices** 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

Procedure

Step 1 Log-in to Security Cloud Control using an account with Admin or Super Admin privileges.

Step 2 In left pane, click **Administration** > **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 Security Cloud Control. 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:

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Note
For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **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 Security Cloud Control to the device, preview and deploy 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 Security Cloud Control to the device, or you want to "undo" the configuration changes you started making on Security Cloud Control. This option overwrites the configuration stored in Security Cloud Control with the running configuration stored on the device.

Resolve the Conflict Detected Status

Security Cloud Control 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 Security Cloud Control, the device's configuration status will show **Conflict Detected**.

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

Procedure

Step 1 In the navigation bar, click **Security Devices**.

Note
For an On-Premises Firewall Management Center, click **Administration** > **Integrations** > **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 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 Security Cloud Control.
- 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** Security Cloud Control with the device's running configuration.

  Note
  As Security Cloud Control 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 Security Cloud Control.

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,Security Cloud Control polls the device for the default interval to determine if a change has been made to the device's configuration outside of Security Cloud Control. You can customize how often Security Cloud Control 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 **Security Devices** page overrides the polling interval selected as the Default Conflict Detection Interval from the **General Settings** page.

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

Procedure

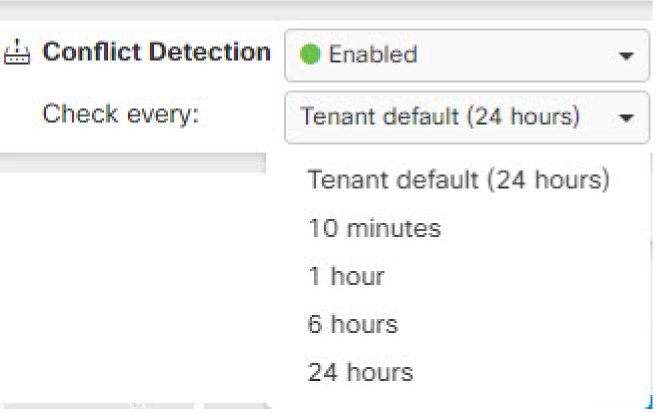
Step 1 In the left pane, click **Security Devices**.

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)