

Manage device configuration

To manage a device, Security Cloud Control stores a copy of the device configuration in its local database. When Security Cloud Control reads a configuration from a managed device, it copies and saves the configuration.

Security Cloud Control also reads and saves a copy of a device configuration when the device is onboarded. Each of these actions serves a specific purpose.

- **Discard Changes**: This action is available when a device configuration status is "Not Synced." In the **Not Synced** state, there are changes to the device configuration pending on Security Cloud Control. This option allows you to undo all pending changes. The pending changes are deleted and Security Cloud Control overwrites its copy of the configuration with the copy of the configuration stored on the device.
- **Check for Changes**: This action is available if the device configuration status is "Synced." Click **Check for Changes** to instruct Security Cloud Control to compare its copy of the device configuration with the copy stored on the device. If a difference is detected, Security Cloud Control immediately overwrites its copy of the device configuration with the copy stored on the device.
- **Review Conflict** and **Accept Without Review**: If you have enabled Conflict Detection on a device, Security Cloud Control checks for configuration changes made on the device every 10 minutes. If the copy of the configuration stored on the device has changed, Security Cloud Control notifies you by displaying the "Conflict Detected" configuration status.
  - **Review Conflict**: Click **Review Conflict** to review changes made directly on a device and accept or reject them.
  - **Accept Without Review**: This action overwrites the copy of the device configuration on Security Cloud Control with the latest copy of the configuration stored on the device. Security Cloud Control 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 any number of devices in any state and click **Read All** to overwrite all the device configurations stored on Security Cloud Control with the configurations stored on the devices.

- **Deploy Changes**: When you make changes to a device configuration, Security Cloud Control saves your changes to its copy of the configuration. These changes remain **Pending** in Security Cloud Control until you deploy them to the device. If there are pending changes that have not been deployed, the device is in the **Not Synced** configuration state.

Pending configuration changes do not affect network traffic. They take effect only after Security Cloud Control deploys them to the device.

When Security Cloud Control deploys changes to a device configuration, only the elements that were changed are overwritten. The entire device configuration file is not overwritten. You can deploy changes to one device or multiple devices simultaneously.

- **Discard All**: This option appears after you click **Preview and Deploy...**. When you click **Preview and Deploy...**, Security Cloud Control displays a preview of the pending changes in Security Cloud Control. You can delete all pending changes from Security Cloud Control without deploying them to the selected devices by clicking **Discard All**. Unlike "Discard Changes," deleting the pending changes completes the operation.



Note You can schedule deployments or recurring deployments. For more information about scheduling an automatic deployment, refer to Schedule an Automatic Deployment, on page 15.

- Read, discard, and deploy configuration changes, on page 2
- Synchronizing configurations between Security Cloud Control and device, on page 20
- Synchronizing configurations between Security Cloud Control and device, on page 28

Read, discard, and deploy configuration changes

Read All Device Configurations

If a configuration change is made to a device outside of Security Cloud Control, the device 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.

For more information about how Security Cloud Control manages the two copies of the device configuration, refer to Reading, Discarding, Checking for, and Deploying Configuration Changes.

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 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.

Procedure

Step 1 Choose **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Click the appropriate device type tab.

Step 4 Select the devices whose configurations you want to save in Security Cloud Control.

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

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.

Step 5 Click **Read All** to continue.

Step 6 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.

Read configuration changes from an ASA to Security Cloud Control

Why does Security Cloud Control "Read" ASA configurations?

To manage an ASA, Security Cloud Control must have its own copy of the ASAs running configuration file. Security Cloud Control reads and saves a copy of the device configuration file for the first time during device onboarding. When Security Cloud Control reads a configuration from an ASA, you can choose to **Check for Changes**, **Accept without Review**, or **Read Configuration**. For more information, refer to Reading, Discarding, Checking for, and Deploying Configuration Changes.

Security Cloud Control also needs to read an ASA configuration in these circumstances:

- When deployment of configuration changes to the ASA fails and the device state is not listed or **Not Synced**.
- When device onboarding fails and the device state is **No Config**.
- When changes are made to the device configuration outside of Security Cloud Control and those changes have not yet been polled or detected. In this case, the device state is **Synced** or **Conflict Detected**.

In these cases, Security Cloud Control needs a copy of the last known configuration stored on the device.

Read configuration changes on ASA device

Read configuration changes on your ASA device by completing these steps when prompted:

Procedure

Step 1 Choose **Inventory**.

Step 2 Choose **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab.

Step 5 Select the device that Security Cloud Control has recently failed to onboard, or select the device where Security Cloud Control could not deploy a change.

Step 6 Click **Read Configuration** in the **Synced** pane. This option overwrites the configuration currently saved to Security Cloud Control.

Read Configuration Changes from FDM-Managed Device to Security Cloud Control

Why Does Security Cloud Control Read FDM-managed device Configurations?

In order to manage an FDM-managed device, Security Cloud Control must have its own stored copy of the FDM-managed device's configuration. When Security Cloud Control reads a configuration from an FDM-managed device, it takes a copy of the FDM-managed device's deployed configuration and saves it to its own database. The first time Security Cloud Control reads and saves a copy of the device's configuration file is when the device is onboarded. See Reading, Discarding, Checking for, and Deploying Configuration Changes for more information.

Pending and Deployed Changes

Configuration changes made to the FDM-managed device directly through the Firepower Device Manager (FDM) or its CLI are referred to as staged changes on the FDM-managed device until they are deployed. A staged, or pending, change can be edited or deleted without having any affect on traffic running through the FDM-managed device. Once the pending changes are deployed, however, they are enforced by the FDM-managed device and affect traffic running through the device.

Conflict Detected

If you enable Conflict Detection on the device, Security Cloud Control checks for configuration changes every 10 minutes. If the copy of the configuration stored on the device has changed, Security Cloud Control notifies you by displaying the "Conflict Detected" configuration status. If you do **not** have Conflict Detection enabled, or a change has been made to the device's configuration within the 10 minute interval between automatic polling, clicking **Check for Changes** prompts Security Cloud Control to immediately compare the copy of the configuration on the device with the copy of the configuration stored on Security Cloud Control. You can choose to **Review Conflict** to examine the differences between the device configuration and the configuration saved to Security Cloud Control, then select **Discard Changes** to remove the staged changes and revert to the saved configuration or confirm the changes. You can also choose to **Accept without Review**; this option takes the configuration and overwrites what is currently saved to Security Cloud Control.

Discard Changes Procedure

To discard configuration changes from the FDM-managed device, follow this procedure:

Procedure

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

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

Step 3 Click the **Devices** tab.

Step 4 Click the appopriate device type tab.

Step 5 Select the device whose configuration is set to Conflict Detected and gives you the link to Revert Pending Changes. The message explains that you can click the link to revert pending changes or you can log on to the device using the local manager FDM and deploy the changes first.

Caution
Clicking the Revert Pending Changes link deletes pending changes on FDM-managed device immediately. You are not given an opportunity to review the changes first.

Step 6 Review the changes on FDM before clicking Revert Pending Changes:

a. Open a browser window and enter https://<*IP_address_of_the_FTD*>.

b. Look for the deployment icon in FDM. It will have an orange circle indicating that there are changes ready to deploy .

c. Click the icon and review the pending changes:

- If the changes can be deleted, return to Security Cloud Control and click "Revert Pending Changes." At this point, the configuration on the FDM-managed device and the copy of the configuration on Security Cloud Control should be the same. You are done.
- If you want to deploy the changes to the device, click **Deploy Now**. Now the deployed configuration on the FDM-managed device and the configuration on stored on Security Cloud Control are different. You can then return to Security Cloud Control and poll the device for changes. Security Cloud Control identifies identifies that there has been a change on the FDM-managed device, and gives you an opportunity to review the conflict. See Conflict Detected-Review Conflict to resolve that state.

If Reverting Pending Changes Fails

Changes to the system databases and security feeds can't be reverted by Security Cloud Control. Security Cloud Control recognizes that there are pending changes, attempts to revert them and then fails. To determine if the revert failure is due to pending database updates or security feed updates, log into the device's FDM console. It will have an orange circle indicating that there are changes ready to deploy . Click the deploy button to review the pending changes and deploy them or discard them as is appropriate.

Review Conflict Procedure

To review configuration changes from the FDM-managed device, follow this procedure:

Procedure

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

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

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab.

Step 5 Select the device whose configuration is marked Conflict Detected and gives you a link to **Review Conflict** in the Conflict Detected pane on the right.

Step 6 Click **Review Conflict.**

Step 7 Compare the two configurations presented to you.

Step 8 Take one of these actions:

- Click **Accept** to overwrite the last known configuration on Security Cloud Control with the one found on the device. **Note**: The entire configuration stored on Security Cloud Control will be completely overwritten by the configuration found on the device.
- Click **Reject** to reject the changes made on the device and replace them with the last known configuration on Security Cloud Control.
- Click **Cancel** to stop the action.

Note
You can prompt Security Cloud Control to immediately check a device for an out-of-band change by clicking Check for Changes while the device is in the Synced state.

Accept Without Review Procedure

To accept configuration changes from the FDM-managed device without reviewing, follow this procedure:

Procedure

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

Step 2 In the left pane, click the **Security Devices** tab.

Step 3 Click the appopriate device type tab.

Step 4 Select the device whose configuration is marked Conflict Detected and gives you a link to **Accept Without Review** in the Conflict Detected pane on the right.

Step 5 Click **Accept Without Review**. Security Cloud Control accepts and overwrites the current configuration.

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 organization, but you have not deployed that change, by displaying an orange dot on the deploy icon . Each device affected by these changes displays a status of "Not Synced" in the **Security Devices** page. Click **Deploy** to 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 a single configuration change. Alternatively, you can 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 displays a yellow caution triangle, you cannot deploy changes to that device. Hover your pointer over the yellow caution triangle to see the reason.

Step 3 (Optional) If you want to see more information about a pending change, click the **View Detailed Change log** 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 that you selected. You will 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. The results of the deployment appear in a recent "Deploy Changes" job.

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

Deploy configuration changes from Security Cloud Control to ASA

Why does Security Cloud Control deploy changes to an ASA?

When you manage and make changes to a device configuration with Security Cloud Control, Security Cloud Control saves those changes to its own copy of the configuration file. Those changes are considered staged on Security Cloud Control until they are deployed to the device. Staged configuration changes have no effect on the network traffic running through the device. Only after Security Cloud Control deploys the changes to the device do they have an effect on the traffic running through the device. When Security Cloud Control deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. These actions do not overwrite the entire configuration file on your device.

The ASA has a running configuration file (sometimes called the running config) and a startup configuration file (sometimes called the startup config). The configuration stored in the running config file is enforced on traffic passing through the ASA. After you change the running config and confirm the device behaves as you want, deploy those changes to the startup config. When you reboot the ASA, it starts using the startup config as its configuration starting point. If you do not save your changes to the startup config, you lose them when you reboot the ASA.

Deploying changes from Security Cloud Control to an ASA writes those changes to the running configuration file. When you are satisfied with how those changes affect the device, deploy them to the startup configuration file.

You can start deployments for one device or several devices simultaneously. You can schedule single or recurring deployments for a device.

Some changes are deployed directly to the ASA

If you use the command line interface on Security Cloud Control to make a change to an ASA, those changes are not staged on Security Cloud Control. They are deployed directly to the running configuration of the ASA. When you make changes that way, your device remains synced with Security Cloud Control.

Deploy configuration changes

This section assumes you are using Security Cloud Control's GUI or editing the Device Configuration page to make changes to an ASA configuration file, and not using Security Cloud Control's CLI interface or CLI macro interface.

To update an ASA configuration, complete these two steps.

Procedure

Step 1 Make changes on Security Cloud Control using one of these methods:

- The Security Cloud Control GUI
- The device configuration on the **Device Configuration** page

Step 2 After you make your changes, return to the **Security Devices** page and select **Preview and Deploy...** to apply the change to the device.

Further you can:

When Security Cloud Control updates an ASA's running configuration with the one staged on Security Cloud Control or changes the configuration on Security Cloud Control with the running configuration stored on the ASA, it attempts to change only the relevant lines of the configuration file. These selective changes occur only if the configuration aspect can be managed by the Security Cloud Control GUI. If the desired configuration change cannot be made using the Security Cloud Control GUI, Security Cloud Control attempts to overwrite the entire configuration file.

Here are two examples:

- You **can** create or change a network object using the Security Cloud Control GUI. If Security Cloud Control needs to deploy that change to an ASA's configuration, it would overwrite the relevant lines of the running configuration file on the ASA when the change occurs.
- You **cannot** create a new local ASA user using the Security Cloud Control GUI but you can create one by editing the ASA's configuration on the Device Configuration page. If you add a user on the Device Configuration page, and you deploy that change to the ASA, Security Cloud Control will try to save that change to the ASA's running configuration file by overwriting the entire running configuration file.

Deploy configuration changes made using the Security Cloud Control GUI

Procedure

Step 1 When you make a configuration change using Security Cloud Control GUI and save it, the change is stored in the version of the ASA's running configuration file kept in Security Cloud Control.

Step 2 Return to the device on the **Security Devices** page.

Step 3 Click the **Devices** tab. The device status now displays **Not synced**.

Step 4 Choose one of these methods to deploy the changes.

- Click the **Deploy** icon ( ) at the top right of the screen. A review screen appears so you can examine your changes. Select the device you modified, expand it to review the changes, and click **Deploy now** to deploy the changes.

  Note
  If you see a yellow warning triangle next to your device on the **Devices with Pending Changes** screen, you cannot deploy changes to it. Hover over the warning triangle to learn why you cannot deploy changes.

- In the **Not Synced** pane, click **Preview and Deploy...**

  a. Review the commands that will change the ASA configuration file.

  b. If you are satisfied with the commands, choose a **Configuration Recovery Preference**.

  Note
  If you choose **Let me know and I will restore the configuration manually**, click **View Manual Synchronization Instructions** before continuing.

  c. Click **Apply Changes to Device**.

  d. Click **OK** to acknowledge the success message.

Schedule automatic deployments

You can configure your tenant to deploy changes automatically either to a single device or to all devices with pending changes. For more information about the deployment scheduling feature, refer to scheduling automatic deployments.

Deploy configuration changes using Security Cloud Control's CLI interface

Procedure

Step 1 Choose **Inventory**.

Step 2 Choose **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab.

Step 5 Select the device whose configuration you want to change.

Step 6 Click **>_Command Line Interface** in the **Actions** pane.

Step 7 If there are any commands in the command line interface table, click **Clear** to remove them.

Step 8 In the top box of the command line interface table, enter your commands at the command prompt. You can run a single command, several commands in a batch by entering each command on its own line, or entering a section of configuration file as a command. Here are some examples of commands you can enter in the command line interface table.

A single command creating the network object "albany"

```
object network albany
host 209.165.30.2
```

Multiple commands sent together:

```
object network albany
host 209.165.30.2
object network boston
host 209.165.40.2
object network cambridge
host 209.165.50.2
```

A section of a running configuration file entered as a command:

```
interface GigabitEthernet0/5
 nameif guest
 security-level 0
 no ip address
```

Note
Security Cloud Control does not require you to move between EXEC mode, Privileged EXEC mode, and Global Configuration mode. It interprets the command you enter in the proper context.

Step 9 After you have entered your commands, click **Send**. After Security Cloud Control has successfully deployed the changes to the ASA's running config file, you receive the message, Done!

Step 10 After you send the command, you may see the message, "Some commands may have made changes to the running config." This message includes two links.

- Click **Deploy to Disk** to save the changes made by this command, and any other change in the running config, to the ASA's startup config.
- Click **Dismiss** to dismiss the message.

Deploy configuration changes by editing the device configuration



Caution This procedure is for advanced users who are familiar with the syntax of an ASA configuration file. This method makes changes directly to the running configuration file stored on Security Cloud Control.

Procedure

Step 1	Choose **Security Devices**
Step 2	Choose **Inventory**.
Step 3	Click the appropriate device type tab.
Step 4	Select the device whose configuration you want to change.
Step 5	Click **View Configuration** in the **Actions** pane.
Step 6	Click **Edit**.
Step 7	Make your changes to the running configuration and **Save** them.
Step 8	Return to the **Security Devices** page. In the Not Synced pane, click **Preview and Deploy...**
Step 9	In the **Device Sync** pane to review the changes.
Step 10	Click **Replace Configuration** or **Apply Changes to Device** depending on the kind of change it is.

Deploy Configuration Changes for a Shared Object on Multiple Devices

Use this procedure when you are making changes to a policy or object shared by two or more devices. You can change a common policy on however many devices use it.

Procedure

Step 1	Open and edit the Policies page or the Objects page containing the shared object you want to edit.
Step 2	Review the shared device list and confirm that you want to make the changes on all the devices mentioned.
Step 3	Click **Confirm**.
Step 4	Click **Save**.
Step 5	Click the **Deploy** icon and deploy your changes to the affected devices.

Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device

Why Does Security Cloud Control Deploy Changes to an FDM-Managed Device?

As you manage and make changes to a device's configuration with Security Cloud Control, Security Cloud Control saves the changes you make to its own copy of the configuration file. Those changes are considered staged on Security Cloud Control until they are deployed to the device. Staged configuration changes have no effect on the network traffic running through the device. Only after Security Cloud Control deploys the changes to the device do they have an affect on the traffic running through the device. When Security Cloud Control deploys changes to the device's configuration, it only overwrites those elements of the configuration that were changed. It does not not overwrite the entire configuration file stored on the device.

Like Security Cloud Control, FDM-managed device has the concept of pending changes and deployed changes. Pending changes on FDM-managed device are the equivalent of staged changes on Security Cloud Control. A pending change can be edited or deleted without having any affect on traffic running through the FDM-managed device. Once the pending changes are deployed, however, they are enforced by the FDM-managed device and affect traffic running through the device.

Because of FDM-managed devices two step process for editing configuration files, Security Cloud Control deploys changes to an FDM-managed device slightly differently than it does to other devices it manages. Security Cloud Control first deploys the changes to FDM-managed device and the changes are in the pending state. Then, Security Cloud Control deploys the changes on the devices and they become live. Now that the changes have been deployed, they are enforced and affect traffic running through the FDM-managed device. This applies to both standalone and high availability (HA) devices.

Deployments can be initiated for a single device or on more than one device simultaneously. You can schedule individual deployments or recurring deployments for a single device.

Two things will prevent Security Cloud Control from deploying changes to an FDM-managed device:

- If there are staged changes on the FDM-managed device. See Conflict Detected for more information on how to resolve this state.
- Security Cloud Control does not deploy changes if there are changes in the process of being deployed to the FDM-managed device.

Scheduling Automatic Deployments

You can also configure your tenant to schedule deployments to a single device with pending changes scheduling automatic deployments.

Deploy Changes to a Device

Procedure

Step 1 When you make a configuration change for a device using Security Cloud Control and save it, that change is saved in the Security Cloud Control instance of the device configuration.

Step 2 Choose **Inventory**.

Step 3 Choose **Security Devices**.

Step 4 Click the **Devices** tab.

Step 5 Click the appropriate device type tab. The configuration status of the device will display "Not synced" after you make changes.

Step 6 To deploy the changes, select one of these methods:

- Select the device and in the "Not Synced" pane, and click **Preview and Deploy**. On the Pending Changes screen, review the changes. If you are satisfied with the pending version, click **Deploy Now**.
- Click the **Deploy** icon . For more information, refer to Preview and deploy configuration changes for all devices, on page 7.

Cancelling Changes

If, when deploying a change from Security Cloud Control 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 Security Cloud Control 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. Security Cloud Control 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:

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, such as changing a value or adding an override to an object, you can deploy all those changes at once to your on-premises Firewall Management Center.

Note This task deploys configuration changes only to on-premises Firewall Management Center. To deploy these changes to your Firewall Threat Defense devices, you must deploy these changes manually from your on-premises Firewall Management Center. For more information, see Configuration Deployment in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Procedure

Step 1 Choose **Tools & Services** > **Firewall Management CenterAdministration** > **Integrations** > **Firewall Management Center**

Step 2 Click the **FMC** tab.

Step 3 Select the on-premises Firewall Management Center where you want to preview and deploy changes.

Note
Security Cloud Control identifies when your on-premises Firewall Management Center is out of sync and displays the status as **Not Synced**.

Step 4 Click **Preview and Deploy** on the details pane.

Step 5 Review any warnings. To deploy immediately, click **Deploy Now**. If you do not want to proceed, click **Discard All**.

Step 6 Alternatively, click the download button at the top-right corner of the screen to open the **Devices with Pending Changes** window. Select the devices, review the pending changes on the selected devices, and then deploy them.

Step 7 Click **Deploy Now** to deploy the changes.

About Scheduled Automatic Deployments

Using Security Cloud Control, 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.

If there were changes made directly to the device that have not been read to Security Cloud Control, 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.

Enable scheduled automatic deployments

Enabling the option to schedule automatic deployments allows you to schedule future deployments at a date and time when it is convenient. Once you enable this option, you can schedule a single automatic deployment or set up recurring automatic deployments.

Changes you make on Security Cloud Control for a device are not automatically deployed to the device if it has pending changes . If a device is not in the **Synced** state, such as **Conflict Detected** or **Not Synced**, scheduled deployments are not executed. The jobs page lists any instance where a scheduled deployment fails.

If you turn off **Enable the Option to Schedule Automatic Deployments**, all scheduled deployments are deleted.

Important If you use Security Cloud Control to create more than one scheduled deployment for a device, the new deployment overwrites the existing deployment. If you create more than one scheduled deployment for a device using the API, you **must** delete the existing deployment before scheduling the new deployment.

Follow these steps to enable scheduled automatic deployments:

Procedure

Step 1 Choose **Settings** > **General Settings**.

Step 2 Choose **Administration** > **General Settings**.

Step 3 Turn on the **Enable the option to schedule automatic deployments** toggle button to enable it.

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.

Important This procedure applies only to ASAs and FDM-managed devices.

To schedule deployments for Secure Firewall Threat Defense devices managed by on-premises Firewall Management Center or Cloud-Delivered Firewall Management Center, see Scheduling.

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

Procedure

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

Step 2 From the Security Cloud Control home page, choose **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab.

Step 5 Select one ore more devices.

Step 6 In the Device Details pane, locate the Scheduled Deployments tab and click **Schedule**.

Step 7 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 8 Click **Save**.

Edit a Scheduled Deployment

Follow this procedure to edit a scheduled deployment:

Procedure

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

Step 2 From the Security Cloud Control home page, choose **Security Devices**.

Step 3 Click the **Devices** tab.

Step 4 Click the appropriate device type tab.

Step 5 Select one or more devices.

Step 6 In the **Device Details** pane, locate the Scheduled Deployments tab and click **Edit** .



Step 7 Edit the recurrence, date, or time of a scheduled deployment.

Step 8 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.

Procedure

Step 1 Choose **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** .

- Reading, Discarding, Checking for, and Deploying Configuration Changes
- Read All Device Configurations, on page 2
- Deploy configuration changes from Security Cloud Control to ASA, on page 7
- Deploy Configuration Changes from Security Cloud Control to FDM-Managed Device, on page 11
- Preview and deploy configuration changes for all devices, on page 7

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 Security Cloud Control. You will see the this option when the device is in the "Synced" state.

To check changes:

Procedure

Step 1 From the Security Cloud Control home page, choose **Security Devices**.

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 FTD 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 Security Cloud Control.
- Click **Cancel** to cancel the action.

- For ASA device:

a. Compare the two configurations presented to you. Click **Continue**. The configuration labeled **Last Known Device Configuration** is the configuration stored on Security Cloud Control. 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 Security Cloud Control 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 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 From the Security Cloud Control home page, choose **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.

Discard On-Premises Firewall Management Center configuration changes

To undo all configuration changes you made in Security Cloud Control, such as changes to objects shared between your Security Cloud Control and on-premises Firewall Management Center, follow this procedure. When you perform this task, Security Cloud Control *completely overwrites* its local configuration copy with the configuration stored on the device.

Procedure

Step 1 Choose **Tools & Services** > **Firewall Management CenterAdministration** > **Integrations** > **Firewall Management Center**.

Step 2 Click the **FMC** tab.

Step 3 Select the on-premises Firewall Management Center for which you want to discard changes.

Step 4 Click **Discard Changes** in the **Not Synced** pane.

When you click **Discard Changes**, your on-premises Firewall Management Center configuration status changes to **Not Synced**. After you discard your changes, the configuration copy stored in Security Cloud Control matches the configuration on on-premises Firewall Management Center. The status in Security Cloud Control then 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 Firewall Management Center, Security Cloud Control declares the on-premises Firewall 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 24 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

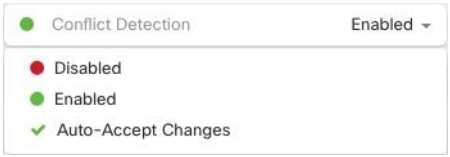
Step 1 Choose **Security Devices**.

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.



Enable conflict detection for an On-Premises Firewall Management Center

Enabling conflict detection for an on-premises Firewall Management Center keeps you informed when there are changes made outside Security Cloud Control that are pending synchronization with Security Cloud Control, and when there are changes made in Security Cloud Control that are pending deployment to on-premises Firewall Management Center.

Procedure

Step 1 Choose **Tools & Services** > **Firewall Management CenterAdministration** > **Integrations** > **Firewall Management Center**.

Step 2 From the list, select the on-premises Firewall 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 Firewall 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 Firewall 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 20 instead.

Configure Auto-Accept Changes

Procedure

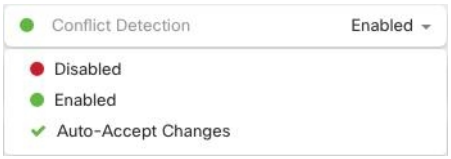
Step 1 Log in to Security Cloud Control using an account with Admin or Super Admin privileges.

Step 2 Choose **Settings** > **General SettingsAdministration** > **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 Choose **Settings** > **General SettingsAdministration** > **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 explains how to resolve 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 Choose **Inventory**.

Note
For an On-Premises 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 Choose **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 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select the device reported as Not Synced.

Step 6 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 20 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 Choose **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 enable Conflict Detection, on page 20 or **Enable the option to auto-accept device changes** from the **Settings** page, Security Cloud Control polls the device at the default interval to check for configuration changes

made outside Security Cloud Control. You can set how often Security Cloud Control polls for changes for each device. This customization can be applied to multiple devices.

If you do not configure a selection for a device, the interval is automatically configured for "tenant default".

After you enable **Conflict Detection** from the **Security Devices** page or **Enable the option to auto-accept device changes** from the **Settings** page, you can schedule how often Security Cloud Control polls your devices with this procedure.

Procedure

Step 1 Choose **Inventory**.

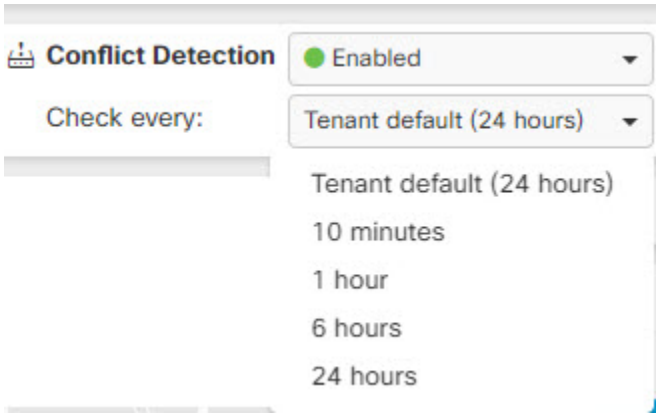
Step 2 Choose **Security Devices**.

Step 3 Click the **Devices** tab to locate your device.

Step 4 Click the appropriate device type tab.

Step 5 Select the devices where you want to enable conflict detection.

Step 6 Next to **Conflict Detection**, click the drop-down menu for **Check every** and select the polling interval you want.



Schedule a Security Database Update

This section provides information about scheduling a security database update on the device.

Create a Scheduled Security Database Update

Use the following procedure to create a scheduled task to check and update the security databases for an FDM-managed device:

Procedure

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

Step 2 In the navigation bar, click **Security Devices**.

Step 3 Click the **Devices** tab to locate your device.

Step 4 Click the **FTD** tab.

Step 5 Select a device.

Step 6 In the **Actions** pane, locate the **Security Database Updates** section and click the**add +** button.

Note

If there is an existing scheduled task for the selected device, click the edit icon to create a new task. Creating a new task will overwrite the existing one.

Step 7 Configure the scheduled task with the following:

- **Frequency** . Choose for the update to occur daily, weekly, or monthly.
- **Time**. Choose the time of day. Note that the time displayed is UTC.
- **Select Days.** Choose which day(s) of the week you want the update to occur.

Step 8 Click **Save**.

The device's Configuration Status will change to "Updating Databases".

Edit a Scheduled Security Database Update

Use the following procedure to edit an existing scheduled task to check and update the security databases for an FDM-managed device.

Procedure

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

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

Step 3 Click the **FTD** tab.

Step 4 Select a device.

Step 5 In the **Actions** pane, locate the **Security Database Updates** section and click the edit icon .

Step 6 Edit the scheduled task with the following:

- **Frequency** . Choose for the update to occur daily, weekly, or monthly.
- **Time**. Choose the time of day. Note that the time displayed is UTC.
- **Select Days.** Choose which day(s) of the week you want the update to occur.

Step 7 Click **Save**.

Step 8 The device's Configuration Status will change to "Updating Databases".

Update FDM-Managed Device Security Databases

By updating the security databases on an FDM-managed device, you are updating the following: SRUs (intrusion rules), security intelligence (SI), vulnerability databases (VDB), and geolocation databases. If you opt into updating the security databases through the Security Cloud Control UI, note that **all** of the mentioned databases are updated; you cannot select which databases you want to update.

Please note that security database updates cannot be reverted.

Note When you update the security databases, some packets may be dropped or pass uninspected. We recommend you schedule your security database updates during a maintenance window.

Update FDM-Managed Device Security Database While Onboarding

When you onboard an FDM-managed device to Security Cloud Control, part of the onboarding process allows you to **Enable scheduled recurring updates for databases**. This option is checked by default. When enabled, Security Cloud Control immediately checks for and applies any security updates as well as automatically schedules the device to check for additional updates. You are able to modify the date and time of the scheduled task after the device is onboarded.

Update FDM-Managed Device Security Database After Onboarding

After an FDM-managed device is onboarded to Security Cloud Control, you can configure a device to check for security database updates by scheduling an update. You can modify this scheduled task at any time by selecting the device the update is scheduled for. See Schedule a Security Database Update for more information.

Workflows

Device licenses

Security Cloud Control cannot update the security databases if there is no license. We recommend that your FDM-managed device has at least an license.

If you are onboarding a device that has no license, this does not inhibit Security Cloud Control from onboarding the device. Instead, the device will experience a **Connectivity** status of "insufficient licenses". To resolve this issue, you must apply the correct licenses through the FDM-managed device UI.

Note If you onboard an FDM-managed device and opt in to schedule future security database updates and the device does **not** have a registered license, Security Cloud Control still creates the scheduled task but does not trigger the task until the appropriate licenses have been applied and the device is successfully synchronized.

Security database updates are pending in FDM

If you update the security databases through the FDM-managed device UI, and you have **conflict detection** enabled on your device, Security Cloud Control detects the pending update as a conflict.

Note If you onboard your FDM-managed device and opt to schedule the updates, Security Cloud Control automatically updates the security databases as well as any other pending changes to the stored configuration during the next deploy. **does not have to be a configuration deploy**

Device has OOB changes, or staged changes, during a security database update

If you schedule a security database update for an FDM-managed device that has out of band (OOB) changes, or staged changes that have not been deployed, Security Cloud Control only checks and updates the security databases. Security Cloud Control does **not** deploy OOB or staged changes.

Device already has a scheduled task to update the security databases

Each device can only have one scheduled task. If the device already has a scheduled task to update the security databases, creating a new one overwrites it. This applies to tasks that are created in either Security Cloud Control or an FDM-managed device.

No security database updates available

If there are no updates available, Security Cloud Control does not deploy anything to the device.

Security database updates for FDM-managed High Availability (HA) pair

Security database updates are applied only to the primary device of an HA pair.

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 Firewall Management Center, Security Cloud Control declares the on-premises Firewall 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 24 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

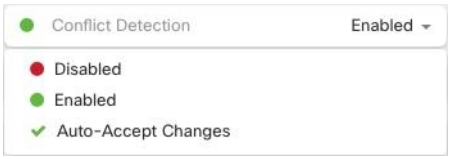
Step 1 Choose **Security Devices**.

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.



Enable conflict detection for an On-Premises Firewall Management Center

Enabling conflict detection for an on-premises Firewall Management Center keeps you informed when there are changes made outside Security Cloud Control that are pending synchronization with Security Cloud Control, and when there are changes made in Security Cloud Control that are pending deployment to on-premises Firewall Management Center.

Procedure

Step 1 Choose **Tools & Services** > **Firewall Management CenterAdministration** > **Integrations** > **Firewall Management Center**.

Step 2 From the list, select the on-premises Firewall 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 Firewall 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 Firewall 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 20 instead.

Configure Auto-Accept Changes

Procedure

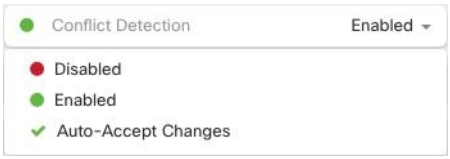
Step 1 Log in to Security Cloud Control using an account with Admin or Super Admin privileges.

Step 2 Choose **Settings** > **General SettingsAdministration** > **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 Choose **Settings** > **General SettingsAdministration** > **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 explains how to resolve 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 Choose **Inventory**.

Note
For an On-Premises 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 Choose **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 3 Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.

Step 4 Click the appropriate device type tab.

Step 5 Select the device reported as Not Synced.

Step 6 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 20 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 Choose **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 enable Conflict Detection, on page 20 or **Enable the option to auto-accept device changes** from the **Settings** page, Security Cloud Control polls the device at the default interval to check for configuration changes made outside Security Cloud Control. You can set how often Security Cloud Control polls for changes for each device. This customization can be applied to multiple devices.

If you do not configure a selection for a device, the interval is automatically configured for "tenant default".

After you enable **Conflict Detection** from the **Security Devices** page or **Enable the option to auto-accept device changes** from the **Settings** page, you can schedule how often Security Cloud Control polls your devices with this procedure.

Procedure

Step 1 Choose **Inventory**.

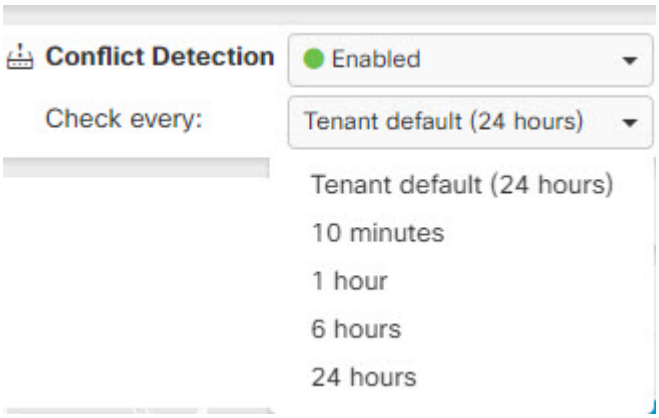
Step 2 Choose **Security Devices**.

Step 3 Click the **Devices** tab to locate your device.

Step 4 Click the appropriate device type tab.

Step 5 Select the devices where you want to enable conflict detection.

Step 6 Next to **Conflict Detection**, click the drop-down menu for **Check every** and select the polling interval you want.



Schedule a Security Database Update

This section provides information about scheduling a security database update on the device.

Create a Scheduled Security Database Update

Use the following procedure to create a scheduled task to check and update the security databases for an FDM-managed device:

Procedure

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

Step 2 In the navigation bar, click **Security Devices**.

Step 3 Click the **Devices** tab to locate your device.

Step 4 Click the **FTD** tab.

Step 5 Select a device.

Step 6 In the **Actions** pane, locate the **Security Database Updates** section and click the**add +** button.

Note

If there is an existing scheduled task for the selected device, click the edit icon to create a new task. Creating a new task will overwrite the existing one.

Step 7 Configure the scheduled task with the following:

- **Frequency** . Choose for the update to occur daily, weekly, or monthly.
- **Time**. Choose the time of day. Note that the time displayed is UTC.
- **Select Days.** Choose which day(s) of the week you want the update to occur.

Step 8 Click **Save**.

The device's Configuration Status will change to "Updating Databases".

Edit a Scheduled Security Database Update

Use the following procedure to edit an existing scheduled task to check and update the security databases for an FDM-managed device.

Procedure

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

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

Step 3 Click the **FTD** tab.

Step 4 Select a device.

Step 5 In the **Actions** pane, locate the **Security Database Updates** section and click the edit icon .

Step 6 Edit the scheduled task with the following:

- **Frequency** . Choose for the update to occur daily, weekly, or monthly.
- **Time**. Choose the time of day. Note that the time displayed is UTC.
- **Select Days.** Choose which day(s) of the week you want the update to occur.

Step 7 Click **Save**.

Step 8 The device's Configuration Status will change to "Updating Databases".

Update FDM-Managed Device Security Databases

By updating the security databases on an FDM-managed device, you are updating the following: SRUs (intrusion rules), security intelligence (SI), vulnerability databases (VDB), and geolocation databases. If you opt into updating the security databases through the Security Cloud Control UI, note that **all** of the mentioned databases are updated; you cannot select which databases you want to update.

Please note that security database updates cannot be reverted.

Note When you update the security databases, some packets may be dropped or pass uninspected. We recommend you schedule your security database updates during a maintenance window.

Update FDM-Managed Device Security Database While Onboarding

When you onboard an FDM-managed device to Security Cloud Control, part of the onboarding process allows you to **Enable scheduled recurring updates for databases**. This option is checked by default. When enabled,

Security Cloud Control immediately checks for and applies any security updates as well as automatically schedules the device to check for additional updates. You are able to modify the date and time of the scheduled task after the device is onboarded.

Update FDM-Managed Device Security Database After Onboarding

After an FDM-managed device is onboarded to Security Cloud Control, you can configure a device to check for security database updates by scheduling an update. You can modify this scheduled task at any time by selecting the device the update is scheduled for. See Schedule a Security Database Update for more information.

Workflows

Device licenses

Security Cloud Control cannot update the security databases if there is no license. We recommend that your FDM-managed device has at least an license.

If you are onboarding a device that has no license, this does not inhibit Security Cloud Control from onboarding the device. Instead, the device will experience a **Connectivity** status of "insufficient licenses". To resolve this issue, you must apply the correct licenses through the FDM-managed device UI.



Note If you onboard an FDM-managed device and opt in to schedule future security database updates and the device does **not** have a registered license, Security Cloud Control still creates the scheduled task but does not trigger the task until the appropriate licenses have been applied and the device is successfully synchronized.

Security database updates are pending in FDM

If you update the security databases through the FDM-managed device UI, and you have **conflict detection** enabled on your device, Security Cloud Control detects the pending update as a conflict.



Note If you onboard your FDM-managed device and opt to schedule the updates, Security Cloud Control automatically updates the security databases as well as any other pending changes to the stored configuration during the next deploy. **does not have to be a configuration deploy**

Device has OOB changes, or staged changes, during a security database update

If you schedule a security database update for an FDM-managed device that has out of band (OOB) changes, or staged changes that have not been deployed, Security Cloud Control only checks and updates the security databases. Security Cloud Control does **not** deploy OOB or staged changes.

Device already has a scheduled task to update the security databases

Each device can only have one scheduled task. If the device already has a scheduled task to update the security databases, creating a new one overwrites it. This applies to tasks that are created in either Security Cloud Control or an FDM-managed device.

No security database updates available

If there are no updates available, Security Cloud Control does not deploy anything to the device.

Security database updates for FDM-managed High Availability (HA) pair

Security database updates are applied only to the primary device of an HA pair.