

Configure On-Premises Firewall Management Center-Managed Threat Defense Devices

This chapter provides steps to configure On-Premises Firewall Management Center-managed Threat Defense devices.

- View onboarded On-Premises Firewall Management Center, on page 1
- Discover and manage On-Premises Firewall Management Center network objects, on page 2
- Preview and deploy On-Premises Firewall Management Center configurations, on page 3
- Discard On-Premises Firewall Management Center configuration changes, on page 4

View onboarded On-Premises Firewall Management Center

To view onboarded On-Premises Firewall Management Centers, perform these steps:

1. Choose **Tools & Services** > **Firewall Management CenterAdministration** > **Integrations** > **Firewall Management Center**.
2. Click the **FMC** tab.

View On-Premises Firewall Management Center high-availability pair

The high-availability pair is displayed in the **Services** page. When you expand the pair, you can see the primary and secondary on-premises Firewall Management Center nodes and their current statuses.

To cross-launch the active on-premises Firewall Management Center, perform these steps:

1. In the **Services** page, check the corresponding high-availability pair.
2. Click the option you want to open in on-premises Firewall 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 Firewall Management Center is shown and will be used to open on-premises Firewall Management Center. If necessary, specify the URL of the standby on-premises Firewall Management Center to launch it.

Add cross-launch URLs to each on-premises Firewall Management Center node. When you launch from the pair, only the active node is launches. Verifying which node is currently active is not necessary.

To cross-launch to a specific on-premises Firewall Management Center node, perform these steps:

1. Expand the high-availability pair and click primary or secondary on-premises Firewall Management Center node you want to launch.
2. In the **External Links** pane, click **FMC Cross Launch URL** to cross-launch the selected on-premises Firewall Management Center.

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

Note If high availability is broken or roles are switched on on-premises Firewall Management Center (version 7.4.x or earlier), disable the SecureX integration, then enable it again on the secondary on-premises Firewall Management Center. To complete this task, navigate to the secondary on-premises Firewall Management Center and choose the appropriate option.

If you break a high-availability on-premises Firewall Management Center pair, the participating management centers become two standalone on-premises Firewall Management Centers.

Discover and manage On-Premises 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, perform this procedure:

Procedure

Step 1 Choose **Tools & Services** > **Firewall Management CenterAdministration** > **Integrations** > **Firewall Management Center** to view the **Services** page.

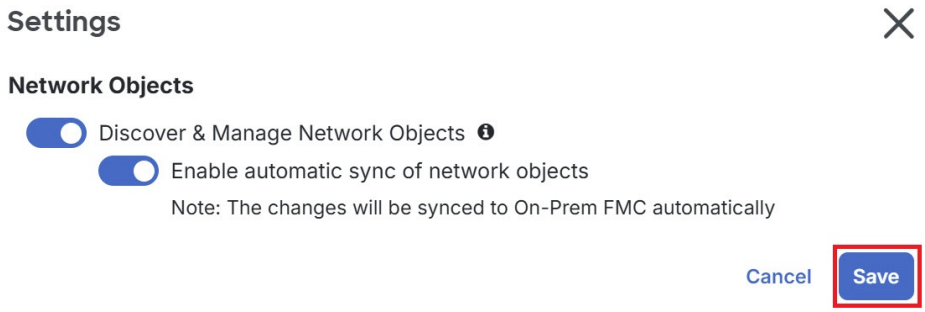
Step 2 If you have already onboarded an on-premises Firewall Management Center to Security Cloud Control, select it.

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

Step 3 Choose **Settings** from the **Actions** pane. The **Actions** pane does not appear when you select more than one on-premises Firewall Management Center.

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

Step 4 Enable the **Discover & Manage Network Objects** toggle button. To automatically synchronize your changes with on-premises Firewall Management Center instead of staging them for review, turn on the **Enable automatic sync of network objects** toggle button. Then, click **Save**.



Note

- You cannot enable the **Discover & Manage Network Objects** toggle button if the selected on-premises Firewall Management Center has one or more child domains or if it has the Change Management workflow enabled.
- You cannot enable the **Enable automatic sync of network objects** toggle button if the **Discover & Manage Network Objects** toggle button is disabled.

For every new on-premises Firewall Management Center onboarded to Security Cloud Control, this toggle button needs to be enabled manually. After you enable this option, Security Cloud Control discovers objects from your on-premises Firewall Management Center. You can then share and manage these objects, and use them 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 Firewall Management Center and push the changes back, these objects can now be overridden, even if overrides were not allowed previously. The **Allow Overrides** check box in the **View Network Object** window is selected 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 Firewall Management Center, choose the on-premises Firewall Management Center and click **Assign Objects** from the **Actions** pane.

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.

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**.