

Onboard an On-Premises Firewall Management Center

This chapter provides steps to onboard an On-Premises Firewall Management Center and manage associated Threat Defense devices.

- Onboard an On-Premises Firewall Management Center to Security Cloud Control Firewall Management, on page 1
- Remove an On-Premises Firewall Management Center from Security Cloud Control, on page 4

Onboard an On-Premises Firewall Management Center to Security Cloud Control Firewall Management

Security Cloud Control Firewall Management provides two methods to onboard on-premises Firewall Management Centers.

- Use on-premises Firewall Management Center credentials with SDC is supported but intended only for very rare use cases. Onboarding with SDC limits access to many cloud assist features available with direct onboarding. Choose SDC if direct onboarding is not possible.

Security Cloud Control complements FMC by enabling:

- Consistent policy enforcement through shared object management with FMCs.
- Zero-touch provisioning of Firewall Threat Defense devices. For more information, refer to Onboard a Device to On-Premises Firewall Management Center with Zero-Touch Provisioning.
- Centralized visibility and management of security devices. For more information, refer to Device and Service Management.
- Integration with cloud Cisco Secure Dynamic Attributes Connector (CSDC) and Cloud-Delivered Firewall Management Center. For more information, refer to Cisco Secure Dynamic Attributes Connector.

Limitations and Guidelines

- Onboarding an on-premises Firewall Management Center also onboards all devices registered to it. Disabled or unreachable devices may appear in the **Security Devices** page in Security Cloud Control but cannot be managed or queried.

- Onboarding does **not** cascade policies from on-premises Firewall Management Center to Security Cloud Control or Cloud-Delivered Firewall Management Center. To migrate Firewall Threat Defense devices to Cloud-Delivered Firewall Management Center, use the built-in **Migrate FTD to** Cloud-Delivered Firewall Management Center feature. For more information, refer to Migrate Threat Defense to Cloud-delivered Firewall Management Center.
- We recommend creating a dedicated user on the on-premises Firewall Management Center with administrator-level permissions specifically for Security Cloud Control communication. If you log in to on-premises Firewall Management Center with the same credentials during onboarding, the process will fail. This recommendation applies only to credentials-based onboarding, not to direct integration.
- For this dedicated user, set the **Maximum Number of Failed Logins** to zero.
- For on-premises Firewall Management Centers version 7.4 or later, if a switchover causes a loss of cloud connectivity, disable and then re-enable **SecureX**, **Security Cloud Control**, or **Cisco Security Cloud** (depending on your version) to restore the connection.

Onboard an On-Premises Firewall Management Center to Security Cloud Control with Credentials

To onboard an on-premises Firewall Management Center to Security Cloud Control with credentials, follow this procedure:

Before you begin

These prerequisites must be met:

- **For Cloud Secure Device Connector (SDC)**: Allow inbound traffic on port 443 of the on-premises Firewall Management Center.

  The SDC reaches the on-premises Firewall Management Center by allowing inbound traffic on port 443.



  Both the Security Cloud Control and the SDC are hosted in the cloud.

- **For On-Premises Secure Device Connector (SDC)**: Allow outbound connectivity on port 443 of the SDC.

  The SDC requires connectivity to the Security Cloud Control, making it imperative to permit outbound traffic from the SDC to the Security Cloud Control. No additional port configuration is required on on-premises Firewall Management Center.



Procedure

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

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

Step 3 Click  to onboard an on-premises Firewall Management Center.

Step 4 Click **Firewall Management Center**.

Step 5 Select the **Use Credentials** card.

Step 6 Enter the device name and location and click **Next**.

Step 7 Enter the **Username** and **Password** of the account credentials you want to use to access the on-premises Firewall Management Center. Click **Next**.

Step 8 After you onboard the device, you can add labels to your on-premises Firewall Management Center, or you can click **Go to Services** to view the page of onboarded devices. If the device is healthy, the FMC displays a **Synced** status.

Note
Devices managed by on-premises Firewall Management Center are automatically named as "<*fmcname*>_<*manageddevicename*>."

Redirect Security Cloud Control to an On-Premises Firewall Management Center

After you onboard an on-premises Firewall Management Center to Security Cloud Control, update the management interface's hostname in the on-premises Firewall Management Center UI so that it contains the FQDN. If you do not update the management interface's hostname, you cannot cross-launch from Security Cloud Control.

Use this procedure to update the management interface hostname and redirect from Security Cloud Control to on-premises Firewall Management Center:

Procedure

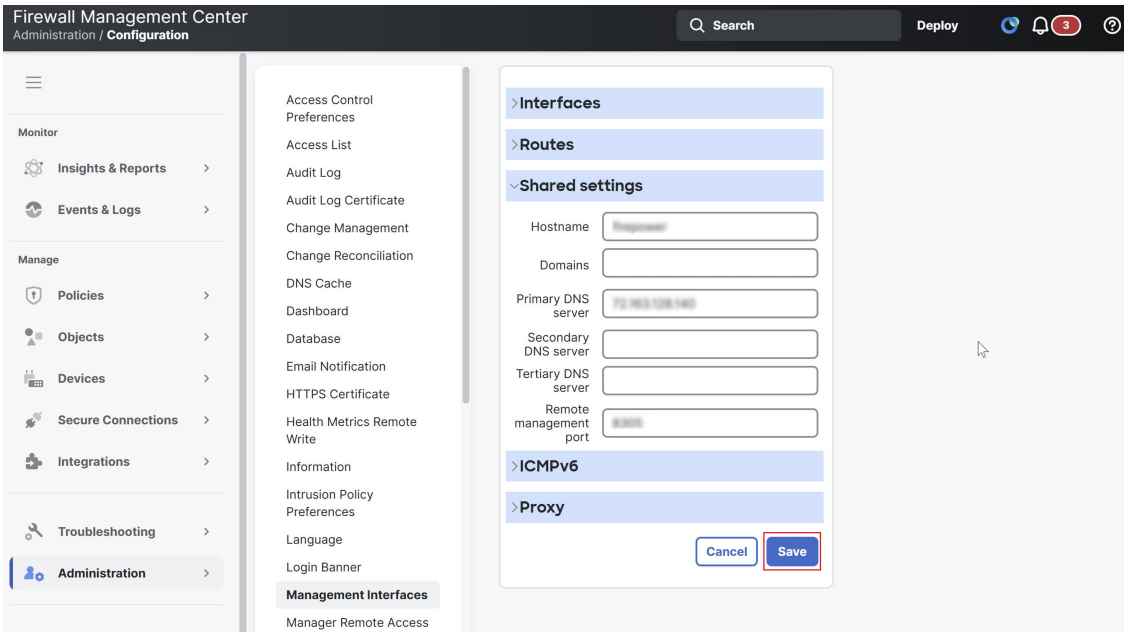
Step 1 Log in to the On-Premises Firewall Management Center UI.

Step 2 Choose **Administration** > **Configuration**.

Step 3 Click the **Management Interfaces** tab.

Step 4 Under **Shared Settings**, locate the **Hostname** field and enter the Firewall Management Center's FQDN.

Step 5 Click **Save**.



Note
You may have to log out of Security Cloud Control before you can click **Manage Devices in Firepower Management Center** and cross-launch to the on-premises Firewall Management Center UI.

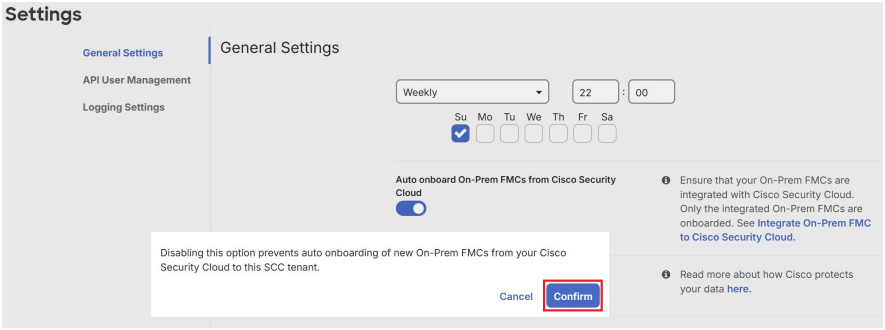
Remove an On-Premises Firewall Management Center from Security Cloud Control

If you remove an on-premises Firewall Management Center from Security Cloud Control, all devices managed by that on-premises Firewall Management Center will also be removed.

Before you begin

To remove one or more on-premises Firewall Management Centers that were onboarded using auto-onboarding, first disable the auto-onboarding option.

1. Choose **Settings** > **General Settings**.
2. Choose **Administration** > **General Settings**.
3. In the **Tenant Settings** section, disable **Auto onboard On-Prem FMCs integrated to Cisco Security Cloud**.



Procedure

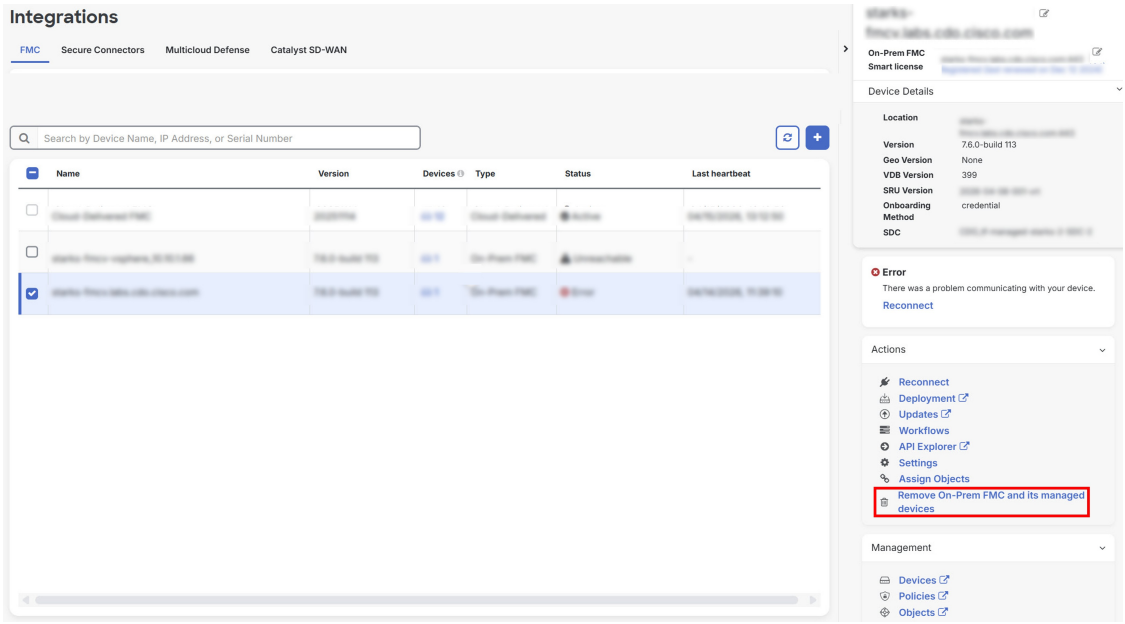
Step 1 Choose **Tools & Services** > **Firewall Management Center**.

Step 2 Choose **Administration** > **Integrations** > **Firewall Management Center**.

Step 3 Click the **FMC** tab.

Step 4 Choose the on-premises Firewall Management Center you want to remove.

Step 5 In the **Device Actions** pane, click **Remove On-Prem FMC and its managed devices**.



Step 6 Click **OK** to confirm that you want to remove on-premises Firewall Management Center and its managed devices from your tenant.

Step 7 Refresh your browser to see an updated list of devices.