



Onboard Devices and Services

You can onboard both live devices and model devices to Security Cloud Control. Model devices are uploaded configuration files that you can view and edit using Security Cloud Control.

Most live devices and services require an open HTTPS connection so that the Secure Device Connector can connect Security Cloud Control to the device or service.

See [Secure Device Connector](#) for more information on the SDC and its state.

This chapter covers the following sections:

- [Onboard an SSH Device, on page 1](#)

Onboard an SSH Device

You can use the username and password of a highly privileged user stored on the SSH device to onboard the device.


Onboard an SSH Device

Before you begin

Before you begin, make sure you have met these prerequisites:

- Ensure that the ciphers your Cisco SSH device supports are supported by Security Cloud Control. At this time, Security Cloud Control supports a limited set of ciphers for onboarding Cisco SSH devices. The supported ciphers are: `aes128-ctr`, `aes192-ctr`, `aes256-ctr`, `aes128-gcm`, `aes128-gcm@openssh.com`, `aes256-gcm`, `aes256-gcm@openssh.com`. To determine the ciphers your server supports, log in to your SDC and run this command: `ssh -vv <ip_address>`.
- You must have an on-premises Secure Device Connector (SDC) in your network to onboard a Cisco IOS device. See [Secure Device Connector](#) for a discussion of SDCs and links to deployment scenarios.
- Before you onboard your device, review [Connect to Cisco Security Cloud Control using Secure Device Connector](#).

Procedure

-
- Step 1** In the left pane, click **Security Devices**.
- Step 2** Click the blue plus button  to onboard a device.
- Step 3** Click the **Integrations** tile. If it is grayed-out, it means you do not have an active Secure Device Connector deployed in your network and used by your Security Cloud Control tenant.
- Step 4** Click the **Secure Device Connector** button and select the SDC in your network that this device will communicate with. The default SDC is displayed but you can change it by clicking the SDC name.
- Step 5** Give the device a name.
- Step 6** In the Integrations drop-down menu, select **Generic SSH**.
- Step 7** Enter the device's location as either the FDQN or IPv4 address. The default SSH port is 22.
- Step 8** Click **Go**. Security Cloud Control locates the device and prepares to integrate the configuration.
- Step 9** **Download** the SSH fingerprint and save locally. If you've never connected to this device through SSH before, this fingerprint allows you to confirm the device.
- Step 10** Enter the Username and Password login credentials for the device you are onboarding. Security Cloud Control cannot successfully read the existing configuration without the correct login information.
- Step 11** (Optional) Enter the **Enable Password** if you've previously configured one for this device.
- Step 12** (Optional) Select a Configuration Command from the drop-down menu, or enter a custom command in the textbox. This command will be used as the configuration for the device; if OOB is enabled, Security Cloud Control checks for changes and you can view the current value of this in the Configuration page. Note that you can change this command once the device is successfully onboarded to Security Cloud Control.
- Step 13** Click **Connect**.
- Note** If the login credentials were incorrect, you will be prompted to review the connection details. Here you can re-enter the login information. If you exit the review without correcting the credentials, the device has an integration instance in the **Inventory** page but the device is not onboarded or synchronized.
- Step 14** (Optional) Add labels to this device.
- Step 15** Click **Continue**.
- Step 16** The device onboards to Security Cloud Control. Click **Finish**.
- Step 17** Return to the **Inventory** page. After the device has been successfully onboarded, you will see that the Configuration Status is "Synced" and the Connectivity state is "Online."
- Note** Once a device is onboarded, you can change the configuration command to be executed. You can use a custom command or create a [CLI macro](#).
- Step 18** (Optional) If you want you can write a note about the device by typing it in the device's Notes page. See [Device Notes](#) for more information.

Related Information:

- [CLI Macros for Managing Devices](#)
-

- [Read Changes from Cisco IOS or SSH to Security Cloud Control](#)
- [Reading, Discarding, Checking for, and Deploying Configuration Changes](#)

Delete a Device from Security Cloud Control

Use the following procedure to delete a device from Security Cloud Control:

Procedure

-
- Step 1** Log into Security Cloud Control.
 - Step 2** In the left pane, click **Security Devices**.
 - Step 3** Locate the device you want to delete and check the device in the device row to select it.
 - Step 4** In the **Device Actions** panel located to the right, select **Remove**.
 - Step 5** When prompted, select **OK** to confirm the removal of the selected device. Select **Cancel** to keep the device onboarded.
-

