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 ASA Device to Security Cloud Control

Use this procedure to onboard a single live ASA device, not an ASA model, to Security Cloud Control. If you want to onboard multiple ASAs at once, see Onboard Multiple ASAs to Security Cloud Control.

Before you begin

Device Prerequisites

- Review Connect Security Cloud Control to your Managed Devices.
- Device must be running at least version 8.4+.

Note TLS 1.2 was not available for the ASA management-plane until version 9.3(2). With version 9.3(2), a local SDC is required to onboard to Security Cloud Control.

- The running configuration file of your ASA must be less than 4.5 MB. To confirm the size of your running configuration file, see Confirming ASA Running Configuration Size.
- IP addressing: Each ASA, ASAv, or ASA security context must have a unique IP address and the SDC must connect to it on the interface configured to receive management traffic.

Certificate Prerequisites

If your ASA device does not have a compatible certificate, onboarding the device may fail. Ensure the following requirements are met:

- The device uses a TLS version equal to or greater than 1.0.
- The certificate presented by the device is not expired, and its issuance date is in the past (i.e. it is already valid, not scheduled to become valid at a later date).
- The certificate must be a SHA-256 certificate. SHA1 certificates are not accepted.
- One of these conditions is true:
  - The device uses a self-signed certificate, and it is the same as the most recent one trusted by an authorized user.
  - The device uses a certificate signed by a trusted Certificate Authority (CA), and provides a certificate chain linking the presented leaf certificate to the relevant CA.

If you experience certificate errors during the onboarding process, see Cannot onboard ASA due to certificate errorfor more information.

Open SSL Cipher Prerequisites

If the device does not have a compatible SSL cipher suite, the device cannot successfully communicate to the Secure Device Connector (SDC). Use any of the following cipher suites:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA256

- DHE-RSA-AES256-SHA256

If the cipher suite you use on your ASA is not in this list, the SDC does not support it and you will need to update the cipher suite on your ASA.

Procedure

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

Step 2 Click the blue plus button  to onboard an ASA.

Step 3 Click the **ASA** tile.

Step 4 In the **Locate Device** step, perform the following:

a. Click the **Secure Device Connector** button and select a Secure Device Connector installed in your network. If you would rather not use an SDC, Security Cloud Control can connect to your ASA using the Cloud Connector. Your choice depends on how you connect Security Cloud Control to your managed devices.

b. Give the device a name.

c. Enter the location (IP address, FQDN, or URL) of the device or service. The default port is 443.

d. Click **Next**.

Step 5 In the **Policy View** step, you will see that **Enable support for onboarding large configurations and enhanced user interface** option is enabled, which allows onboarding large configurations and viewing the new policy view option is enabled. You can disable this option to onboard the device in traditional view and click Next. Note: If you don't see the Policy View step, you can continue to onboard the device in the new policy view.

Step 6 In the **Credentials** step, enter the username and password of the ASA administrator, or similar highest-privilege ASA user, that Security Cloud Control will use to connect to the device and click **Next**.

Step 7 (Optional) In the Done step, enter a label for the device. You will be able to filter your list of devices by this label. See Labels and Label Groups for more information.

Step 8 After labeling your device or service, you can view it in the **Inventory** list.

Note Depending on the size of the configuration and the number of other devices or services, it may take some time for the configuration to be analyzed.

Onboard a High Availability Pair of ASA Devices to Security Cloud Control

When onboarding an ASA that is part of a high-availability pair, use Onboard ASA Device to Security Cloud Control, on page 1 to onboard only the primary device of the pair.

Onboard an ASA in Multi-Context Mode to Security Cloud Control

About Multi-Context Mode

You can partition a single ASA, installed on a physical appliance, into multiple logical devices known as contexts. There are three kinds of configurations used in an ASA configued in multi-context mode:

- Security Context
- Admin Context
- System Configuration

About Security Contexts

Each security context acts as an independent device, with its own security policy, interfaces, and administrators. Multiple security contexts are similar to having multiple standalone devices. A security context is not a virtual ASA in the sense of a virtual machine image installed in a private cloud infrastructure. A security context is configured on an ASA installed on a hardware appliance. Each context is configured on a physical interface of that appliance.

See the ASA CLI and ASDM configuration guides for more information about multi-context mode.

Security Cloud Control onboards each security context as a separate ASA and manages it as if it were a separate ASA.

About Admin Contexts

The admin context is like a security context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way, and can be used as a regular context. However, because logging into the admin context grants you administrator privileges over all contexts, you might need to restrict access to the admin context to appropriate users.

Security Cloud Control onboards each admin context as a separate ASA and manages it as if it were a separate ASA. Security Cloud Control also uses the admin context when upgrading ASA and ASDM software on the appliance.

About System Configuration

The system administrator adds and manages contexts by configuring each context configuration location, allocated interfaces, and other context operating parameters in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the ASA. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the *admin context*.

Security Cloud Control does not onboard the system configuration.

Onboarding Prerequisites for Security and Admin Contexts

The prerequisites for onboarding security and admin contexts are the same for onboarding any other ASA. See Onboard ASA Device to Security Cloud Control, on page 1for the list of prerequisites.

To learn which Cisco appliances support ASAs in multi-context mode, see the "Multiple Context Mode" chapter in the *CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide* for whatever ASA software version you are running.

For an ASA running as a single context firewall and for the admin context of a multiple-context firewall, many different port numbers could be used for ASDM and Security Cloud Control access. However, for security contexts, the ASDM and Security Cloud Control access port is fixed to port 443. This is a limitation of ASA.

Onboarding ASA Security and Admin Contexts

The method of onboarding a security context or admin context is the same for onboarding any other ASA. See Onboard ASA Device to Security Cloud Control, on page 1 or Onboard Multiple ASAs to Security Cloud Control, on page 5 for onboarding instructions.

Upgrading Security Contexts

Security Cloud Control treats each security and admin context of a multiple-context ASA as a separate ASA and each is onboarded separately. However, all security and admin contexts of a multiple-context ASA run the same version of ASA software installed on the appliance.

To upgrade the versions of ASA and ASDM used by the ASA's security contexts, you onboard the the admin context and perform the upgrade on that context. See Upgrade ASA and ASDM Images on a Single ASA, on page 13 or Upgrade Bulk ASA and ASDM in Security Cloud Control, on page 10 Upgrade Bulk ASA and ASDM in Security Cloud Control, on page 10for more information.

Onboard Multiple ASAs to Security Cloud Control

Security Cloud Control allows you to bulk onboard ASAs by providing the necessary information for all the ASAs in a .csv file. As the ASAs are being onboarded, you can use the filter pane to show which onboarding attempts are queued, loading, complete, or have failed.

Before you begin

- Review Connect Security Cloud Control to your Managed Devices.
- Prepare a .csv file with the connection information of the ASAs you want to onboard. Add the information about one ASA on its own line. You can use a # at the beginning of a line to indicate a comment.
  - ASA location (either IP address or FQDN)
  - ASA administrator username
  - ASA administrator password
  - (Optional) Device name for Security Cloud Control
  - In the SDCName field, specify the name of a Secure Device Connector (SDC) in your network you want to use to connect Security Cloud Control to your ASA. You can also enter "none" if you are not going to connect your ASA to Security Cloud Control using an SDC. When onboarding the

device, specifying "none" in SDCName field, onboards the ASA using the Cloud Connector. The Cloud Connector allows you to connect your device to Security Cloud Control without installing an SDC. Your choice depends on how you connect Security Cloud Control to your managed device.

- (Optional) Device labels for Security Cloud Control
- To add one label, add the label name to the last CSV field.
- To add more than one label to a device, surround the values with quotes. For example, `alpha,beta,gamma`.
- To add a category and choice label, separate the two values with a colon (:). For example, `Rack:50`.

Sample of the configuration file:

```
#Location,Username,Password,DeviceName,SDCName,DeviceLabel
192.168.3.2,admin,CDO123!,ASA3,sdc1,"HA-1,Rack:50"
192.168.4.2,admin,CDO123!,ASA4,sdc1,"HA-1,Rack:50"
ASA2.example.com,admin,CDO123!,ASA2,none,Rack:51
asav.virtual.io,admin,CDO123!,ASA-virtual,sdc3,Test
```

Caution Security Cloud Control does not validate any of the data in the .csv file. You need to ensure the accuracy of the entries.

Procedure

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

Step 2 Click the blue plus button  to onboard an ASA.

Step 3 On the Onboarding page, click the **Multiple ASAs** tile.

Step 4 Click **Browse** to locate the .csv file containing your ASA entries. The devices you specified are now queued in the ASA Bulk Onboarding table ready to be onboarded.

Caution Do not navigate away from the ASA Bulk Onboarding page until the onboarding process is complete. Navigating away stops the onboarding process.

Step 5 Click **Start**. You will see the progress of the onboarding process in the status column of the ASA Bulk Onboarding table. After the device have been successfully onboarded you will see their status change to "Complete."

What to do next

If you need to pause bulk onboarding and resume it later, see Pause and Resume Onboarding Multiple ASAs, on page 7

.

Pause and Resume Onboarding Multiple ASAs

If you need to pause the onboarding process, click **Pause**. Security Cloud Control finishes onboarding any device it started onboarding. To resume the bulk onboarding process, click **Start**. Security Cloud Control will start onboarding the next queued device.

If you click **Pause** and navigate away from this page, you will need to return to the page and follow the bulk onboarding procedure again from the beginning. However, Security Cloud Control recognizes the devices it has already onboarded, marks the devices from this new onboarding attempts as duplicates, and quickly moves through the list to onboard the queued devices.

Create and Import an ASA Model to Security Cloud Control

Procedure

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

Step 2 Click the **Devices** tab.

Step 3 Click the **ASA** tab.

Step 4 Select an ASA device and in the **Management** on the left pane, click **Configuration**.

Step 5 Click **Download** to download the device configuration to your local computer.

Import ASA Configuration

Attention: The ASA running configuration file you are onboarding must be less than 4.5 MB. Confirm the size of the configuration file before you onboard it.

Procedure

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

Step 2 Click the blue plus () button to import the configuration.

Step 3 Click on **Import configuration for offline management**.

Step 4 Select the **Device Type** as **ASA**.

Step 5 Click **Browse** and select the configuration file (text format) to upload.

Step 6 Once the configuration is verified, you're prompted to label the device or service. See Labels and Label Groups for more information.

Step 7 After labeling your model device, you can view it in the **Inventory** list.

Note Depending on the size of the configuration and the number of other devices or services, it may take some time for the configuration to be analyzed.

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.

Import Configuration for Offline Device Management

Importing a device's configuration for offline management allows you to review and optimize a device's configuration without having to work on a live device in your network. Security Cloud Control also refers to these uploaded configuration files as "models."

You can import the configurations of these devices to Security Cloud Control:

- Adaptive Security Applicance (ASA). See Create and Import an ASA Model to Security Cloud Control.
- Cisco IOS devices like the Aggregation Services Routers (ASR) and Integrated Services Routers (ISRs).

Prerequisites for ASA and ASDM Upgrade in Security Cloud Control

Security Cloud Control provides a wizard that helps you upgrade the ASA and ASDM images installed on an individual ASA, multiple ASAs, ASAs in an active-standby configuration, and ASAs running in single-context or multi-context mode.

Security Cloud Control maintains a repository of ASA and ASDM images that you can upgrade to. When you choose your upgrade images from Security Cloud Control's image repository, Security Cloud Control performs all the necessary upgrade steps behind the scenes. The wizard guides you through the process of choosing compatible ASA software and ASDM images, installs them, and reboots the device to complete the upgrade. We secure the upgrade process by validating that the images you chose on Security Cloud Control are the ones copied to, and installed on, your ASA. Security Cloud Control periodically reviews its inventory

of ASA binaries and adds the newest ASA and ASDM images to its repository when they are available. This is the best option for customers whose ASAs have outbound access to the internet.

Security Cloud Control's image repository only contains generally available (GA) images. If you do not see a specific GA image in the list, please contact Cisco TAC or email support from the **Contact Support** page. We will process the request using the established support ticket SLAs and upload the missing GA image.

If your ASAs do not have outbound access to the internet, you can download the ASA and ASDM images you want from Cisco.com, store them in your own repository, provide the upgrade wizard with a custom URL to those images, and Security Cloud Control performs upgrades using those images. In this case, however, you determine what images you want to upgrade to. Security Cloud Control does not perform the image integrity check or disk-space check. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB.

Configuration Prerequisites for All ASAs

- DNS needs to be enabled on the ASA.
- ASA should be able to reach the internet if you use upgrade images from Security Cloud Control's image repository.
- Ensure HTTPS connectivity between the ASA and the repository FQDN.
- The ASA has been successfully onboarded to Security Cloud Control.
- The ASA is synced to Security Cloud Control.
- The ASA is online.
- For custom URL upgrades:
  - Use the Cisco ASA Upgrade Guide to determine what version of ASA and ASDM are compatible with your ASAs.
  - Download the ASA and ASDM images to your image repository.
  - Ensure that the ASA has access to your image repository.
  - Ensure you have enough disk space on your ASA for your ASA and ASDM images.
  - Read Upgrade an ASA or ASDM Using Your Own Image for URL syntax information.

Configuration Prerequisites for Firepower 1000 and Firepower 2100 Series Devices

- The FXOS mode of a Firepower 2100 series device must be configured for **appliance** mode. See Set the Firepower 2100 to Appliance or Platform Mode for more information.
- The device must be running ASA Version 9.13(1) or later.
- You must upgrade the FXOS bundle prior to upgrading the ASA software. See Firepower 2100 ASA and FXOS Compatibility for more information.

Firepower 4100 and Firepower 9300 Series Devices Running ASA

Security Cloud Control does not support the upgrade for the Firepower 4100 or Firepower 9300 series devices. You must upgrade these devices outside of Security Cloud Control.

Upgrade Guidelines

- Security Cloud Control can upgrade ASAs configured as an Active/Standby "failover" pair. Security Cloud Control cannot upgrade ASAs configured in an Active/Active "clustered" pair.

Software and Hardware Prerequisites

Minimum ASA and ASDM versions from which you can upgrade:

- ASA: ASA 9.1.2
- ASDM: There is no minimum version.

Supported Hardware Versions

- See ASA Software and Hardware Support.

Upgrade Bulk ASA and ASDM in Security Cloud Control

Procedure

Step 1 Review Prerequisites for ASA and ASDM Upgrade in Security Cloud Control for upgrade requirements and important information about upgrading ASA and ASDM images.

Note If you are upgrading an ASA 1000 or 2000 series device, be sure to read Prerequisites for ASA and ASDM Upgrade in Security Cloud Control.

Step 2 (Optional) In the left pabe, click **Security Devices**.

Step 3 Create a change request label to identify the devices upgraded by this action in the change log.

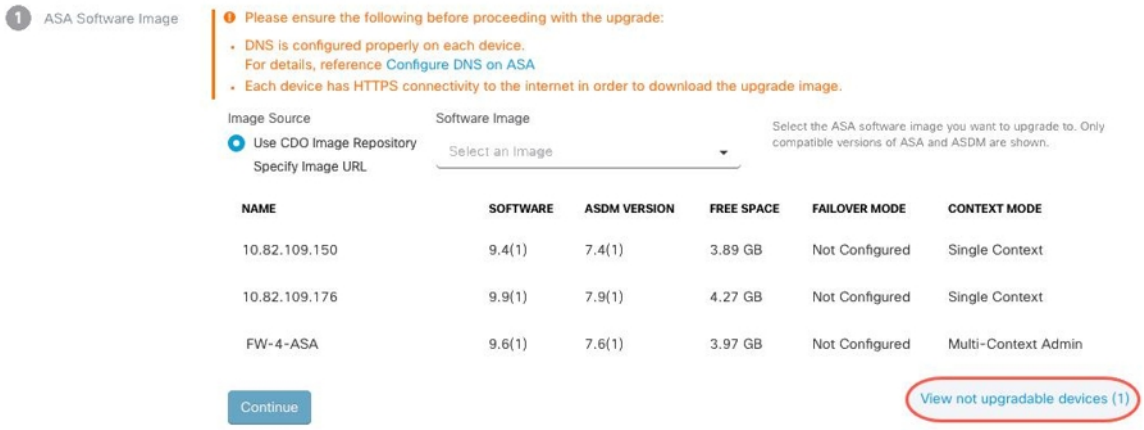
Step 4 Click the **Devices** tab.

Step 5 Use the filter to narrow down the list of devices you may want to include in your bulk upgrade.

Step 6 From the filtered list of devices, select the devices you want to upgrade.

Step 7 In the **Device Actions** pane, click **Upgrade**.

Step 8 On the Bulk Device Upgrade page, the devices that can be upgraded are presented to you. If any of the devices you chose are not upgradable, Security Cloud Control gives you a link to view the not upgradable devices.



Step 9 In step 1, click **Use** Security Cloud Control **Image Repository** to select the ASA software image you want to upgrade to, and click **Continue**.

The list indicates how many of the ASAs you chose can be upgraded to the software version you chose. In the example below, all of the devices can be upgraded to version 9.9(1.2), two devices can be upgraded to 9.8(2), and one of the devices can be upgraded to 9.6(1).

Security Cloud Control alerts you if any of the software versions you chose are incompatible with any of the devices you chose. In the example below, Security Cloud Control cannot upgrade the 10.82.109.176 device to a version earlier thanitalreadyruns.

NAME	SOFTWARE	ASDM VERSION	FREE SPACE	FAILOVER MODE	CONTEXT MODE
✔ 10.82.109.150	9.4(1)	7.4(1)	3.89 GB	Not Configured	Single Context
✔ FW-4-ASA	9.6(1)	7.6(1)	3.97 GB	Not Configured	Multi-Context Admin
✖ 10.82.109.176	9.9(1)	7.9(1)	4.27 GB	Not Configured	Single Context

Step 10 In step 2, select the ASDM image you want to upgrade to. You are only presented with ASDM choices that are compatible with the ASA you can upgrade.

Step 11 In step 3, confirm your choices and decide whether you only want to download the images to your ASAs or copy the images, install them, and reboot the device.

Step 12 Click **Perform Upgrade** when you are ready.

Note If the upgrade fails, Security Cloud Control displays a message. Often the reason for a failed upgrade is a network issue preventing the ASA and ASDM images from being transferred to the ASA.

Step 13 Alternatively, if you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.

Step 14 (For multi-context mode) After the admin context and the security contexts boot, you may see that the security contexts display the message, "New certificate detected." If you see that message, accept the certificate for all security contexts. Accept any other changes caused by the upgrade.

Step 15 Look at the notifications tab for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the Jobs page.

Step 16 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.

Upgrade Multiple ASAs with Images from your own Repository

Procedure

Step 1 Review Prerequisites for ASA and ASDM Upgrade in Security Cloud Control for upgrade requirements and important information about upgrading ASA and ASDM images.

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

Step 3 Create a change request label to identify the devices upgraded by this action in the change log.

Step 4 Click the **Devices** tab.

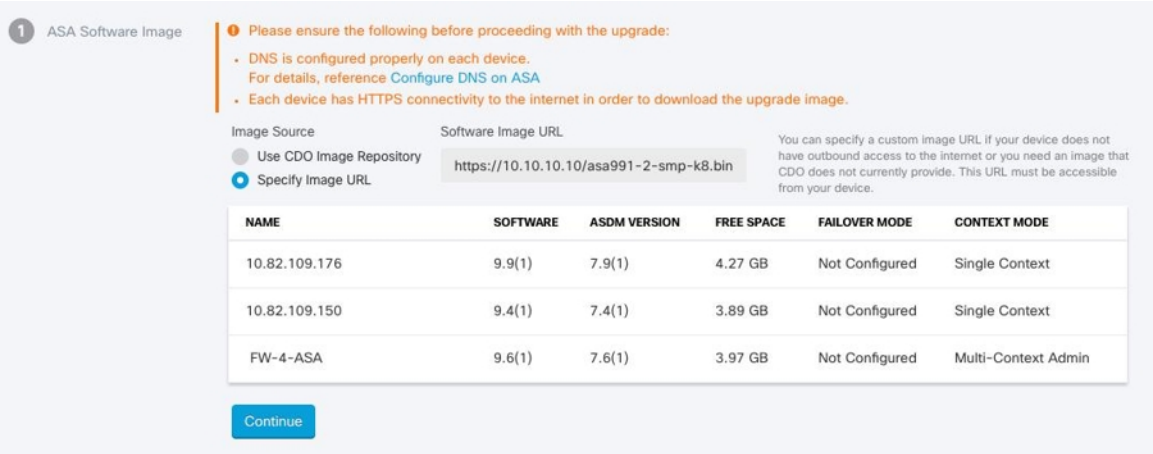
Step 5 Use the Filters to narrow down the list of devices you may want to include in your bulk upgrade.

Step 6 From the filtered list of devices, select the devices you want to upgrade.

Step 7 In the **Device Actions** pane, click **Upgrade**.

Step 8 In step 1, click **Specify Image URL,** enter the URL to the ASA image you want to upgrade to in the In the **Software Image URL** field, and click **Continue**. See Upgrade an ASA or ASDM Using Your Own Image for URL syntax information.

Note The picture below shows an HTTPS URL in the Software Image URL field. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB. See Upgrade an ASA or ASDM Using Your Own Image for URL syntax information.



Step 9 In step 2, click **Specify Image URL,** enter the URL to the ASDM image you want to upgrade to in the In the **Software Image URL** field, and click **Continue**.

Step 10 In step 3, confirm your choices and decide whether you only want to download the images to your ASAs or copy the images, install them, and reboot the device.

Step 11 Click **Perform Upgrade** when you are ready.

Note If the upgrade fails, Security Cloud Control displays a message. Often the reason for a failed upgrade is a network issue preventing the ASA and ASDM images from being transferred to the ASA.

Step 12 Alternatively, if you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.

Step 13 (For multi-context mode) After the admin context and the security contexts boot, you may see that the security contexts display the message, "New certificate detected." If you see that message, accept the certificate for all security contexts. Accept any other changes caused by the upgrade.

Step 14 Look at the notifications tab for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the Jobs page.

Step 15 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.

What to do next

Upgrade Notes

- You can also monitor the progress of the batch of upgrades by opening the **Inventory** page and viewing the Configuration Status column in the table.
- You can view the progress of a single device that was included in the bulk upgrade by selecting that device on the **Inventory** page and clicking the upgrade button. Security Cloud Control takes you to the Device Upgrade page for that device.

Upgrade ASA and ASDM Images on a Single ASA

Follow this procedure to upgrade the ASA and ASDM images on a single ASA.

Procedure

Step 1 Review Prerequisites for ASA and ASDM Upgrade in Security Cloud Control for upgrade requirements and important information about upgrading ASA and ASDM images.

Note If you are upgrading an ASA 1000 or 2000 series device, be sure to read Prerequisites for ASA and ASDM Upgrade in Security Cloud Control.

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

Step 3 Click the **Devices** tab.

Step 4 (Optional) Create a change request label to identify the device upgraded by this action in the change log.

Step 5 Select the device you want to upgrade.

Step 6 In the **Device Actions** pane, click **Upgrade**.

Step 7 On the Device Upgrade page, follow the instructions presented to you by the wizard.

a. In step 1, click **Use** Security Cloud Control **Image Repository** to select the ASA software image you want to upgrade to, and click **Continue**.

Note When upgrading your ASAs and ASDMs to images stored in your own repository, select **Specify Image URL** and enter the URL of the ASA or ASDM image in the Software Image URL field. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB. See Upgrade an ASA or ASDM Using Your Own Image for URL syntax information.

(Optional) If you want Security Cloud Control to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click **Schedule Upgrade**.

b. In step 2, select the ASDM image you want to upgrade to. You are only presented with ASDM choices that are compatible with the ASA you can upgrade.

c. In step 3, confirm your choices and decide whether you only want to download the images to your ASAs or copy the images, install them, and reboot the device.

Step 8 Click **Perform Upgrade** when you are ready.

Step 9 (For multi-context mode) After the admin context and the security contexts boot, you may see that the security contexts display the message, "New certificate detected." If you see that message, accept the certificate for all security contexts. Accept any other changes caused by the upgrade. Want to see a demo? Watch a screencast of this procedure!

What to do next

Upgrade Notes

- If you select an image to upgrade to, and you change your mind, check the **Skip Upgrade** check box associated with the software image. The image will not be copied to the device, nor will the device be upgraded with the image.
- In the **Perform Upgrade** step, if you choose only to copy the images to the ASA, you can return to the Device Upgrade page later and click "Upgrade Now" to perform the upgrade. After the copying task is complete, you will see the message "Ready to Upgrade" for that device on the **Inventory** page.
- You cannot take action on a device during the process of copying the image, installing it, and rebooting the device. Devices that are installing the image and then rebooting are shown as "Upgrading" in the **Inventory** page.
- You cannot take action on a device during the upgrade process; that is, installing the image and rebooting the device.
- You can take action on a device if you choose only to copy the images to the device. Devices that are copying images are shown as "Copying Images" in the **Inventory** page.
- Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information.

Upgrade ASA and ASDM Images in a High Availability Pair

Before you upgrade your pair of ASAs in active/standby failover mode, review the prerequisites below. If you need more information about how ASAs are configured and work in failover mode, see Failover for High Availability in the ASA documentation.

Want to see a demo? Watch a screencast of this procedure.

Prerequisites

- Review Prerequisites for ASA and ASDM Upgrade in Security Cloud Control for requirements and important information about upgrading ASA and ASDM images.
- The primary (active) and secondary (standby) ASAs are configured in active/standby failover mode.
- The primary ASA is the active device in the active/standby pair. If the primary ASA is inactive, Security Cloud Control will not perform the upgrade.
- The primary and secondary ASA software versions are the same.

Workflow

This is the process by which Security Cloud Control upgrades the active/standby pair of ASAs:

Procedure

Step 1 Security Cloud Control downloads the ASA and ASDM images to both ASAs.

Note Users have the choice of downloading ASA and ASDM images but not upgrading immediately. If the ASA and ASDM images were downloaded previously, Security Cloud Control will not download them again; Security Cloud Control continues the upgrade workflow with the next step.

Step 2 Security Cloud Control upgrades the secondary ASA first.

Step 3 Once the upgrade is complete and the secondary ASA returns to the "Standby-Ready" state, Security Cloud Control initiates a failover so that the secondary ASA becomes the active ASA.

Step 4 Security Cloud Control upgrades the primary ASA, which is now the current standby ASA.

Step 5 Once the primary ASA returns to the "Standby-Ready" state, Security Cloud Control initiates a failover so that the primary ASA becomes the active ASA.

Warning Upgrading devices that have self-signed certificates may experience issues; see New Certificate Detected for more information.

Upgrade ASA and ASDM Images in a High Availability Pair

Procedure

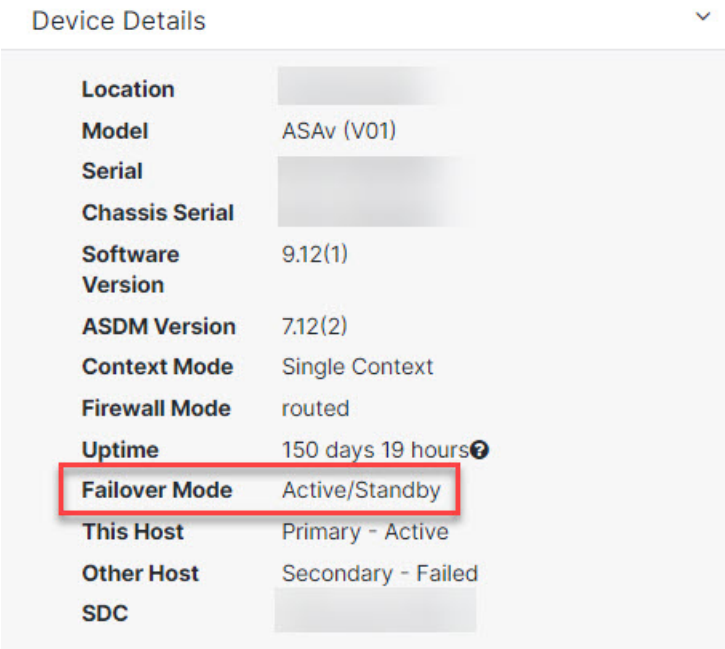
Step 1 In the left pane, click **Security Devices**.

Step 2 Click the **Devices** tab.

Step 3 Select the device you want to upgrade.

Step 4 In the **Device Actions** pane, click **Upgrade**.

Notice that the failover mode of the device is Active/Standby:



Step 5 On the Device Upgrade page, follow the instructions presented to you by the wizard.

Note When upgrading your ASAs and ASDMs to images stored in your own repository, select **Specify Image URL** and enter the URL of the ASA or ASDM image in the Software Image URL field. You can retrieve the images from your repository using any of these protocols: FTP, TFTP, HTTP, HTTPS, SCP, and SMB. See Upgrade an ASA or ASDM Using Your Own Image for URL syntax information.

Upgrade an ASA or ASDM Using Your Own Image

When you upgrade your ASA with new ASA software and ASDM images, you can either use images that Security Cloud Control stores in its image repository or you can use images that you store in your own image repository. If your ASA does not have outbound access to the internet, maintaining your own image repository is the best option for upgrading your ASAs using Security Cloud Control.

Security Cloud Control uses ASA's copy command to retrieve the image and copy it to the flash drive (disk0:/) of your ASA. In the Specify Image URL field you are providing the URL portion of the copy command. For example, if the whole copy command would have been:

```
ciscoasa# copy ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin disk:/0
```

You are providing:

```
ftp://admin:adminpass@10.10.10.10/asa991-smp-k8.bin
```

in the Specify Image URL field.

Security Cloud Control supports http, https, ftp, tftp, smb, and scp methods of retrieving the upgrade image.

URL Syntax examples

Here are examples of URL syntax for the ASA copy command. For the sake of these URL examples, assume the following:

- **Image repository address**: 10.10.10.10
- **Username to access the image repository**: admin
- **Password**: adminpass
- **Path**: images/asa
- **Image filename**: asa991-smp-k8.bin

http[**s**]**://** [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename*]

https://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin
HTTP[s] example without a username and password:
https://10.10.10.10:8080/images/asa/asa991-smp-k8.bin

ftp:// [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename* [**;type=** *xx*]]â€”The **type** can be one of these keywords: **ap** (ASCII passive mode),**an** (ASCII normal mode), **ip**(Defaultâ€”Binary passive mode), **in** (Binary normal mode).

ftp://admin:adminpass@10.10.10.10:20/images/asa/asa991-smp-k8.bin
FTP example without a username and password:
ftp://10.10.10.10:20/images/asa/asa991-smp-k8.bin

tftp:// [[*user* [**:** *password*] **@**] *server* [**:** *port*] **/** [*path* **/**] *filename* [**;int=** *interface_name*]]

tftp://admin:adminpass@10.10.10.10/images/asa/asa991-smp-k8.bin outside
TFTP example without a username and password:
tftp://10.10.10.10/images/asa/asa991-smp-k8.bin outside

Note The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **copy tftp** command. The **;int=** *interface* option bypasses the route lookup and always uses the specified interface to reach the TFTP server.

smb:/[[*path* **/**] *filename*] - Indicates a UNIX server local file system.

smb:/images/asa/asa991-smp-k8.bin

scp:// [[*user* [**:** *password*] **@**] *server* [**/** *path*] **/** *filename* [**;int=** *interface_name*]]â€"The**;int=** *interface* option bypasses the route lookup and always uses the specified interface to reach the Secure Copy (SCP) server.

scp://admin:adminpass@10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside

SCP example without a username and password:

scp://10.10.10.10:8080/images/asa/asa991-smp-k8.bin outside

The complete copy command with URL syntax in the Cisco ASA Series Command Reference, A - H Commands guide.

See Prerequisites for ASA and ASDM Upgrade in Security Cloud Control for more information about upgrading ASA and ASDM images using a custom URL.