



Onboard Secure Firewall ASA

This chapter explains the various different methods using which a Secure Firewall ASA can be onboarded.

- [Onboard Secure Firewall ASA, on page 1](#)

Onboard Secure Firewall ASA

This chapter explains the various different methods using which a Secure Firewall ASA can be onboarded.

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 ASAs in Bulk](#).

Before you begin

Device Prerequisites

- 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.
- 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.

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

Procedure

-
- Step 1** In the navigation bar, click **Inventory**.
- Step 2** In the left pane, click **Security Devices**.
- Step 3** Click the **Onboard device or service** (.
- Step 4** Click the **ASA** tile.
- Step 5** In the **Locate Device** step, perform the following:
- a. Give the device a name.
 - b. Enter the location (IP address, FQDN, or URL) of the device or service. The default port is 443.
 - c. Click **Next**.
- 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 After labeling your device or service, you can view it in the **Security Devices** 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 configured 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 1](#) for 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 4](#) 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 admin context and perform the upgrade on that context.

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

- 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
- (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 navigation bar, click **Inventory**
- Step 2** In the left pane, click **Security Devices**.
- Step 3** Click the blue plus button  to onboard an ASA.
- Step 4** On the Onboarding page, click the **Multiple ASAs** tile.
- Step 5** 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 6** 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 6](#)

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 navigation bar, click **Inventory**.
 - Step 2** In the left pane, click **Security Devices**.
 - Step 3** Click the **Devices** tab.
 - Step 4** Click the **ASA** tab.
 - Step 5** Select an ASA device and in the **Management** on the left pane, click **Configuration**.
 - Step 6** 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 navigation bar, click **Inventory**.
- Step 2** In the left pane, click **Security Devices**.
- Step 3** Click the blue plus (+) button to import the configuration.
- Step 4** Click on **Import configuration for offline management**.
- Step 5** Select the **Device Type** as **ASA**.
- Step 6** Click **Browse** and select the configuration file (text format) to upload.
- Step 7** After labeling your model device, you can view it in the **Security Devices** 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.

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 Appliance (ASA). See [Create and Import an ASA Model](#).
- Cisco IOS devices like the Aggregation Services Routers (ASR) and Integrated Services Routers (ISRs).

FDM Software Upgrade Paths

Upgrading FDM Versions

If you use Security Cloud Control to upgrade your FDM-managed firewalls, Security Cloud Control determines which version you can upgrade to and you will not need this topic. If you maintain your own repository of FDM images and upgrade your FDM-managed devices using your own images, this topic explains what upgrade paths are available to you.

You can upgrade an FDM-managed device directly from one major or maintenance version to another; for example, Version 6.4.0 > 6.5.0, or Version 6.4.0 > 7.0.1. You do not need to be running any specific patch level.

If direct upgrade is not possible, your upgrade path must include intermediate versions, such as Version 6.4.0 > 7.0.0 > 7.1.0.

Table 1: Upgrade Paths for Major Releases

Target Version	Oldest Release you can Upgrade to the Target Version
7.3.x	7.0.0
7.2.x	6.6.0
7.1.x	6.5.0
7.0.x	6.4.0
6.7.x	6.4.0
6.6.x	6.4.0
6.5.0	6.4.0

Patching FDM-Managed Devices

You cannot upgrade directly from a patch of one version to a patch of another version, such as from Version 6.4.0.1 > 6.5.0.1. You must upgrade to the major release first, and then patch that release. For example you must upgrade from Version 6.4.0.1 > 6.5.0 > 6.5.0.1.

Firepower Hotfixes

Security Cloud Control does not support hotfix updates or installations. If there is a hotfix available for your device model or software version, we strongly recommend using the configured manager's dashboard or UI. After a hotfix is installed on the device, Security Cloud Control detects out of band configuration changes.

Removing FDM Upgrades

You cannot use Security Cloud Control to remove or downgrade any release type, whether major, maintenance, or patch.

Starting with Secure Firewall Threat Defense Version 6.7.0, you can use Firepower Device Manager or the FTD CLI to revert a successfully upgraded device to its state just before the last major or maintenance upgrade (also called a snapshot). Reverting after patching necessarily removes patches as well. After reverting, you must reapply any configuration changes you made between **upgrading** and reverting. **Note that to revert a major or maintenance upgrade to FDM Version 6.5.0 through 6.6.x, you must reimage.** See the "System Management" section of a [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#) for more information.

Removing FDM Patches

You cannot remove an FDM patch with either Security Cloud Control or FDM. To remove a patch, you must reimage to a major or maintenance release.

Snort Upgrade

Snort is the main inspection engine for the product and is packaged into the Secure Firewall Threat Defense software for your convenience. Version 6.7 introduces an update to the package that you can upgrade to, or revert from, at any time. Although you can switch Snort versions freely, some intrusion rules in Snort 2.0 might not exist in Snort 3.0, and vice versa. We strongly recommend reading about the differences in the Firepower Device Manager Configuration Guide for Version 6.7.0 for more information.

To proceed with upgrading your FDM-managed device to use Snort 3 or to revert from Snort 3 back to Snort 2 from the Security Cloud Control UI, see [Upgrade to Snort 3.0](#) and [Revert From Snort 3.0 for FTD](#) respectively.

Other Upgrade Limitations

2100 Series Devices

Security Cloud Control can upgrade Firepower 2100 series devices only if they are running appliance mode.

- Firepower Threat Defense devices are always in appliance mode.
- ASA devices are appliance mode by default.

To confirm that your Firepower 2100 running ASA is in appliance mode:

Procedure

-
- | | |
|---------------|--|
| Step 1 | Connect your management computer to the console port or connect to the device using SSH. |
| Step 2 | Enter global configuration mode. |
| Step 3 | Run the show fxos mode command, |


```
ciscoasa(config)# show fxos mode
Mode is currently set to appliance
```

What to do next

See the "[Cisco Firepower 2100 Getting Started Guide](#)" for a more detailed discussion of these commands.

4100 and 9300 Series Devices

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

Related Information:

- [FTD Upgrade Prerequisites](#)
- [ASA and ASDM Upgrade Prerequisites](#)
- [Upgrade a Single FDM-Managed Device](#)
- [Upgrade ASA and ASDM Images on a Single ASA](#)
- [Bulk FTD Upgrade](#)
- [Bulk ASA and ASDM Upgrade](#)
- [Upgrade an FDM-Managed High Availability Pair](#)

FDM-Managed Device Upgrade Prerequisites

Security Cloud Control provides a wizard that helps you upgrade the Firewall Device Manager (FDM) images installed on an individual device or an HA pair.

The wizard guides you through the process of choosing compatible 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 FDM-managed device. We strongly recommend the FDM-managed devices you are upgrading have outbound access to the internet.

If your FDM-managed device does not have outbound access to the internet, you can download the image 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.

Configuration Prerequisites

- DNS needs to be enabled on the FDM-managed device. See the "Configuring DNS" section of the **System Administration** chapter of the [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#) for the version your device is running for more information.
- The FDM-managed device should be able to reach the internet if you use upgrade images from Security Cloud Control's image repository.

- The FDM-managed device has been successfully onboarded to Security Cloud Control.
- The FDM-managed device is reachable.
- The FDM-managed device is synced.
 - If you update a device that has pending changes in Security Cloud Control and you do not accept changes, pending changes are lost after the upgrade completes. Best practice is to deploy any pending changes before you upgrade..
 - If you have staged changes in Firewall Device Manager and the device is not synced, the upgrade in Security Cloud Control will fail at an eligibility check.

4100 and 9300 Series Running FTD

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

Software and Hardware Requirements

Security Cloud Control is a cloud management platform. Software updates are released over time and are generally not dependent on hardware.

Devices running Firewall Device Manager software have a recommended upgrade path for optimal performance. See [Firepower Software Upgrade Path](#) for more information.

Upgrade Notes

You cannot deploy changes to a device while it is upgrading.

Related Information:

- [Firepower Software Upgrade Path](#)
- [Upgrade a Single FDM-Managed Device](#)
- [Bulk FDM-Managed Devices Upgrade](#)
- [Upgrade an FDM-Managed High Availability Pair](#)

Upgrade a Single FDM-Managed Device

Before You Begin

Be sure to read through the [FTD Upgrade Prerequisites](#), [Firepower Software Upgrade Path](#), and the Supported Devices, Software, and Hardware by Security Cloud Control before you upgrade.

This document covers any requirements and warnings you should know prior to upgrading to your desired version of Firepower software.

Upgrade A Single FDM-Managed Device with Images from Security Cloud Control's Repository

Use the following procedure to upgrade a standalone FDM-managed device using a software image that is stored in Security Cloud Control's repository:

Procedure

-
- Step 1** In the navigation bar, click **Security Devices**.
- Step 2** Click the **Devices** tab to locate your device..
- Step 3** Click the **FTD** tab.
- Step 4** Select the device you want to upgrade.
- Step 5** In the **Device Actions** pane, click **Upgrade**.
- Step 6** In step 1, click **Use Security Cloud Control Image Repository** to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
- Step 7** In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.
- Step 8** Click **Perform Upgrade** when you are ready. From the **Security Devices** page, devices that are upgrading have a "Upgrade in Progress" configuration status.
- Warning**
If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.
- Step 9** 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 10** 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 11** Upgrade the system databases. You must do this step in Firewall Device Manager. See "Updating System Databases" in [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#), Version 6.4in for more information.
-

Upgrade a Single FDM-Managed Device with Images from your own Repository

Use the following procedure to upgrade a standalone FDM-managed device using a URL protocol to locate a software image:

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 the device you want to upgrade.
- Step 5** In the **Device Actions** pane, click **Upgrade**.

- Step 6** In step 1, click **Specify Image URL** to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
- Step 7** In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.
- Step 8** Click **Perform Upgrade** when you are ready. From the **Security Devices** page, devices that are upgrading have a "Upgrade in Progress" configuration status.
- Warning**
If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.
- Step 9** 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 10** 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 11** Upgrade the system databases. You must do this step in Firewall Device Manager. See [Updating System Databases](#) in [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#), Version 6.4 for more information.

Monitor the Upgrade Process

You can view the progress of your single device by selecting that device on the **Security Devices** page and clicking the upgrade button. Security Cloud Control takes you to the Device Upgrade page for that device.

If the upgrade fails at any point, Security Cloud Control displays a message. Security Cloud Control does not automatically restart the upgrade process.



Warning Upgrading devices that have self-signed certificates may experience issues; see [New Certificate Detected](#) for more information

Bulk FDM-Managed Devices Upgrade

Before You Begin

Be sure to read through the [FDM-Managed Device Upgrade Prerequisites](#), [Firepower Software Upgrade Path](#), and the Supported Devices, Software, and Hardware supported by Security Cloud Control before you upgrade.

This document covers any requirements and warnings you should know prior to upgrading to your desired version of Firepower software.



Note You can only bulk upgrade FDM-managed devices if they are all upgrading to the same software version.

Upgrade Bulk FDM-Managed Devices with Images from Security Cloud Control's Repository

Use the following procedure to upgrade multiple FDM-managed devices using a software image that is stored in Security Cloud Control's repository:

Procedure

-
- | | |
|----------------|--|
| Step 1 | In the left pane, click Security Devices . |
| Step 2 | Click the Devices tab to locate your devices. |
| Step 3 | Click the FTD tab. |
| Step 4 | From the filtered list of devices, select the devices you want to upgrade. |
| Step 5 | In the Device Actions pane, click Upgrade . |
| Step 6 | 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 7 | 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 8 | In step 1, click Use Security Cloud Control Image Repository to select the software image you want to upgrade to. You are only presented with choices that are compatible with the devices you can upgrade. Click Continue . |
| Step 9 | In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device. |
| Step 10 | Click Perform Upgrade when you are ready. From the Security Devices page, devices that are upgrading have a "Upgrade in Progress" configuration status. |
| | Warning
If you decide to cancel the upgrades while in progress, click Abort Upgrade from the Upgrade page. If you cancel the upgrades after it has started, Security Cloud Control does not deploy or poll for changes from the devices. Devices do not roll back to the previous configuration after a canceled upgrade, either. This may cause the devices to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC. |
| Step 11 | 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 12 | Upgrade the system databases. You must do this step in Firewall Device Manager. See Updating System Databases in Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager , for the version your device is running. |
-

Upgrade Bulk FDM-Managed Devices with Images from your own Repository

Use the following procedure to upgrade multiple FDM-managed devices using a URL protocol to locate a software image:

Procedure

-
- Step 1** In the left pane, click **Security Devices**.
- Step 2** Click the **Devices** tab to locate your devices.
- Step 3** Click the **FTD** tab.
- Step 4** From the filtered list of devices, select the devices you want to upgrade.
- Step 5** In the **Device Actions** pane, click **Upgrade**.
- Step 6** 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 7** 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 8** In step 1, click **Specify Image URL** to select the software image you want to upgrade to, and click **Continue**.
- Step 9** In step 2, confirm your choices and decide whether you only want to download the images to your devices or copy the images, install them, and reboot the device.
- Step 10** Click **Perform Upgrade** when you are ready. From the **Security Devices** page, devices that are upgrading have a "Upgrade in Progress" configuration status.
- Warning**
If you decide to cancel the upgrades while in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrades after it has started, Security Cloud Control does not deploy or poll for changes from the devices and the devices do not roll back to the previous configuration. This may cause the devices to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.
- Step 11** 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 12** Upgrade the system databases. You must do this step in Firewall Device Manager. See "Updating System Databases" in [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#), Version 6.4 in for more information.
-

Monitor the Bulk Upgrade Process

You can view the progress of a single device that was included in the bulk upgrade by selecting that device on the **Security Devices** page and clicking the upgrade button. You can also view the progress details by clicking **Jobs** in the left pane and expanding the bulk operation.

If the upgrade fails at any point, Security Cloud Control displays a message. Security Cloud Control does not automatically restart the upgrade process.

Upgrade an FDM-Managed High Availability Pair

Upgrade your HA pair without disrupting traffic; the standby device continues to handle traffic detection while the secondary device is upgraded.

When you upgrade an HA pair, Security Cloud Control executes an eligibility check and copies or identifies the image location before starting the upgrade. The secondary device in a high availability pair upgrades first, even if it is currently the active device; if the secondary device is the Security Cloud Control active device, the paired devices automatically switch roles for the upgrade process. Once the secondary devices successfully upgrade, the devices switch roles, then the new standby device upgrades. When the upgrade completes, the devices are automatically configured so the primary device is active and the secondary device is standby.

We do not recommend deploying to the HA pair during the upgrade process.

Before You Begin

- Deploy all pending changes to the active device before upgrading.
- Ensure there are no tasks running during the upgrade.
- Both devices in the HA pair are healthy.
- Confirm you are ready to upgrade; you cannot rollback to a previous version in Security Cloud Control.

Upgrade an FDM-Managed HA Pair with Images from Security Cloud Control's Repository

Use the following procedure to upgrade an FDM-managed HA pair using a software image that is stored in Security Cloud Control's repository:

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 the HA pair you want to upgrade. |
| Step 5 | In the Device Actions pane, click Upgrade . |
| Step 6 | In step 1, click Use Security Cloud Control Image Repository to select the software image you want to upgrade to, and click Continue . You are only presented with choices that are compatible with the device you can upgrade. |
| Step 7 | In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device. |
| Step 8 | Click Perform Upgrade when you are ready. From the Security Devices page, devices that are upgrading have a "Upgrade in Progress" configuration status. |

Warning

If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or poll changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

- | | |
|---------------|---|
| Step 9 | 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 10** 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 11** Upgrade the system databases. You must do this step in FDM. See "Updating System Databases" in [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#), Version 6.4 in for more information.

Upgrade an FDM-Managed HA Pair with Images from your own Repository

Use the following procedure to upgrade an FDM-managed HA pair using a URL protocol to locate a software image:

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 the HA pair you want to upgrade.
- Step 5** In the **Device Actions** pane, click **Upgrade**.
- Step 6** In step 1, click **Specify Image URL** to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
- Step 7** In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.
- Step 8** Click **Perform Upgrade** when you are ready. From the **Security Devices** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Warning

If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or poll changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

- Step 9** 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 10** 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 11** Upgrade the system databases. You must do this step in Firewall Device Manager. See "Updating System Databases" in [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#), Version 6.4 for more information.

Monitor the Upgrade Process

You can view the progress of your single device by selecting that device on the **Security Devices** page and clicking the upgrade button. Security Cloud Control takes you to the **Device Upgrade** page for that device.

During the upgrade, the system suspends HA while updating system libraries, which includes an automatic deployment, and may not be in a healthy state for the entirety of the upgrade process. This is expected. The device is available for SSH connections during the last part of this process, so if you log in shortly after applying an upgrade, you might see HA in suspended status. If the system experiences issues during the upgrade process and the HA pair appears to be suspended, manually resume HA from the Firewall Device Manager console of the active device.

**Note**

If the upgrade fails at any point, Security Cloud Control displays a message. Security Cloud Control does not automatically restart the upgrade process.

**Warning**

Upgrading devices that have self-signed certificates may experience issues; see [New Certificate Detected](#) for more information.

Upgrade to Snort 3.0

Snort 3 is the latest snort engine, or a powerful preprocessor that uses Open Source Intrusion Prevention System (IPS), available for Firepower Version 6.7 and later. The snort engine uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users and is ideally used as a packet sniffer, a packet logger, or, more traditionally, as a standalone network IPS.

With Snort 3, you can now create custom intrusion policies; every FDM-managed device running Snort 3 has a set of intrusion policies that are pre-defined from Cisco's Talos Intelligence Group (Talos). Snort 3 makes it possible to change these default policies, although we strongly recommend building on top of the base for a more robust policy.

You cannot create custom policies with Snort 2.

Switching from Snort 2 to Snort 3

You can switch Snort versions freely, though some intrusion rules in Snort 2.0 might not exist in Snort 3.0, and vice versa. If you changed the rule action for an existing rule, that change is not preserved if you switch to Snort 3 and then back to Snort 2, or back again to Snort 3. Your changes to rule actions for rules that exist in both versions are preserved. Note that the mapping between rules in Snort 3 and Snort 2 can be one-to-one or one-to-many, so preservation of changes is done on a best-effort basis.

If you choose to upgrade from Snort 2 to Snort 3, please note that upgrading the snort engines is comparable to a system upgrade. We strongly recommend upgrading during a maintenance window to minimize the interruption in traffic monitoring for your network. See [Managing Intrusion Policies \(Snort3\)](#) in the *Firepower Device Manager Configuration Guide* as to how switching snort versions will affect how rules process traffic.



Tip You can filter by Snort version on the **Security Devices** page, and the Details window of a selected device displays the current version running on the device.

Snort 3 Limitations

License Requirements

To allow the snort engine to process traffic for intrusion and malware analysis, you must have the **license** enabled for the FDM-managed device. To enable this license through Firewall Device Manager, log into the Firewall Device Manager UI and navigate to **Device > View Configuration > Enable/Disable** and enable the license.

Hardware Support

The following devices support Snort 3:

- FTD 1000 series
- FTD 2100 series
- FTD 4100 series
- FTD virtual with AWS
- FTD virtual with Azure
- ASA 5500-X Series with FTD

Software Support

Devices **must** be running at least Firewall Device Manager Version 6.7. Security Cloud Control supports Snort 3 functionality for devices running Version 6.7 and later.

For FTD 1000 and 2000 series, see [FXOS bundled support](#) for more information on FXOS patch support.

Configuration Limitations

Security Cloud Control does not support upgrading to Snort 3 if your device has the following configurations:

- Device is not running at least Version 6.7.
- If a device has pending changes. Deploy any changes prior to upgrading.
- If a device is currently upgrading. Do not attempt to upgrade or deploy to the device until the device is synced.
- If a device is configured with a virtual router.



Note If you upgrade or revert the Snort version, the system automatically deploys to implement the changes between Snort 2 intrusion policies and Snort 3 intrusion policies.

Rulesets and Snort 3

Note that Snort 3 does not have full feature support at this time. Security Cloud Control rulesets are not supported on Snort 3 devices. If you simultaneously upgrade a device to Firewall Device Manager 6.7 or

higher, and from Snort 2 to Snort 3, any rulesets configured prior to the upgrade are broken up and the rules in them are saved as individual rules.

Upgrade the Device and the Intrusion Prevention Engine Simultaneously

Security Cloud Control allows you to upgrade the device to Version 6.7 and the Snort 3. Use the following procedure to upgrade the FDM-managed device:

Procedure

-
- Step 1** In the left pane, click **Security Devices**.
- Step 2** Click the **Devices** tab.
- Step 3** Click the **FTD** tab and select the device or devices you want to upgrade.
- Step 4** In the **Devices Actions** pane located to the right, click **Upgrade**.
- Step 5** Set the upgrade toggle to **FTD System Upgrade**.
- FTD System Upgrade
 Intrusion Prevention Engine
- Step 6** (Optional) If you want Security Cloud Control to perform the upgrade later, check the **Schedule Upgrade** check box. Click in the field to select a date and time in the future.
- Step 7** In step 1, select your upgrade method. Either use the Security Cloud Control Image Repository and an image from your own repository:
- **Use Security Cloud Control Image Repository** - Click this option to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
 - **Specify Image URL** - Click this option to select the software image that is currently stored in your own repository, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
- Step 8** In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.
- Step 9** Check **Upgrade to Snort 3 Engine**.
- Step 10** Click **Perform Upgrade** when you are ready. From the **Security Devices** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Warning

If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

Upgrade the Intrusion Prevention Engine

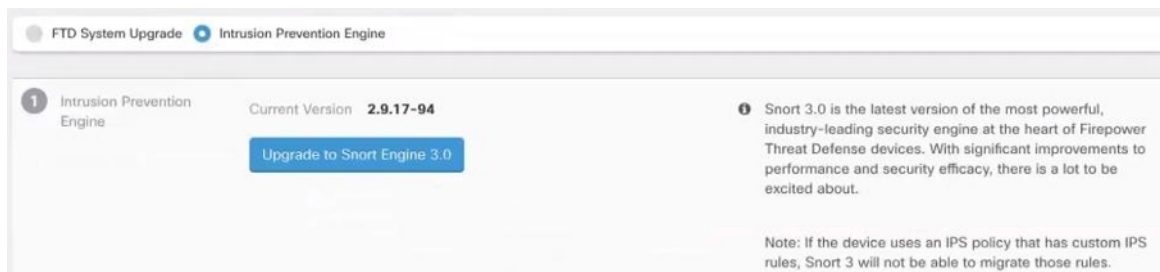
For devices that are already running Version 6.7 with Snort 2, use the following procedure to update just the Snort engine to version 3:

Procedure

- Step 1** In the navigation bar, click **Security Devices**.
- Step 2** Click the **Devices** tab.
- Step 3** Click the **FTD** tab and select the device or devices you want to upgrade.
- Step 4** In the **Device Actions** pane located to the right, click **Upgrade**.
- Step 5** Set the upgrade toggle to **Intrusion Prevention Engine**.



- Step 6** Click **Upgrade to Snort Engine 3.0**.



- Step 7** From the **Security Devices** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Monitor the Upgrade Process



- Warning** If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Security Cloud Control does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

You can view the progress of your single device by selecting that device on the **Security Devices** page and clicking the upgrade button. Security Cloud Control takes you to the **Device Upgrade** page for that device.

If the upgrade fails at any point, Security Cloud Control displays a message. Security Cloud Control does not automatically restart the upgrade process.



- Warning** Upgrading devices that have self-signed certificates may experience issues; see [New Certificate Detected](#) for more information

Revert From Snort 3.0 for FDM-Managed Device

Some intrusion rules in Snort 2.0 might not exist in Snort 3.0. If you downgrade to 2.0, any custom intrusion policies that you created are converted to the base policy used in the custom policy. As far as possible, rule action overrides are retained. If more than one custom policy uses the same base policy, the overrides of the custom policy that is used in the most access control policies are retained, and the overrides for the other custom policies are lost. Access control rules that used these "duplicate" policies will now use the base policy created from your most-used custom policy. All custom policies are deleted.

Before you opt to revert from Snort 3.0, read [Managing Intrusion Policies \(Snort2\)](#) of the *Firepower Device Manager Configuration Guide* and find out how switching snort engine versions will affect your current rules and policies.



Note Reverting to version 2 does not uninstall the Firepower software version.

Revert From Snort 3.0

If you change the Snort version, the system will perform an automatic deployment to implement the change. Note that you can only revert individual devices from Snort 3.0 to version 2.

Use the following procedure to revert the intrusion prevention engine:

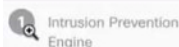
Procedure

- Step 1** In the navigation pane, click **Security Devices**.
- Step 2** Click the **Devices** tab.
- Step 3** Click the **FTD** tab and click the device you want to revert.
- Step 4** In the **Device Actions** pane located to the right, click **Upgrade**.
- Step 5** Set the upgrade toggle to **Intrusion Prevention Engine**.

☐ FTD System Upgrade ☒ Intrusion Prevention Engine

- Step 6** In Step 1, confirm you want to revert from Snort version 3, and click **Revert to Snort Engine 2**.

☐ FTD System Upgrade ☒ Intrusion Prevention Engine



Current Version **3.0.0-269.37**

Revert to Snort Engine 2.0

! Snort 3.0 is the latest version of the most powerful, industry-leading security engine at the heart of Firepower Threat Defense devices. With significant improvements to performance and security efficacy, there is a lot to be excited about.

Note: If the device uses an IPS policy that has custom IPS rules, Snort 3 will not be able to migrate those rules.

- Step 7** From the **Security Devices** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Schedule a 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 left pane, click **Security Devices**.
- Step 2** Click the **Devices** tab.
- Step 3** Click the **FTD** tab and select the desired FDM-managed device.
- Step 4** 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 5** 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 6** Click **Save**.
- Step 7** 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.
- Step 3** Click the **FTD** tab and select the desired FDM-managed device.
- Step 4** In the Actions pane, locate the **Database Updates** section and click the edit icon.
- Step 5** 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 6** Click **Save**.
- Step 7** The device's Configuration Status will change to "Updating Databases".
-

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 [Custom URL Upgrade](#) 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

Upgrade Bulk ASA and ASDM in Security Cloud Control

Procedure

-
- | | |
|---------------|---|
| Step 1 | Review ASA and ASDM Upgrade Prerequisites for upgrade requirements and important information about upgrading ASA and ASDM images. |
| | <p>Note</p> <p>If you are upgrading an ASA 1000 or 2000 series device, be sure to read Configuration Prerequisites for 1000 and 2000 Series.</p> |
| Step 2 | (Optional) In the navigation bar, click Inventory . |
| Step 3 | (Optional) In the left pane, click Security Devices . |
| Step 4 | Click the Devices tab. |
| Step 5 | From the filtered list of devices, select the devices you want to upgrade. |
| Step 6 | In the Device Actions pane, click Upgrade . |

Step 7

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.

1 ASA Software Image

Please ensure the following before proceeding with the upgrade:

- DNS is configured properly on each device. For details, reference [Configure DNS on ASA](#).
- Each device has HTTPS connectivity to the internet in order to download the upgrade image.

Image Source: ☒ Use CDO Image Repository ☐ Specify Image URL

Software Image:

Select the ASA software image you want to upgrade to. Only compatible versions of ASA and ASDM are shown.

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
10.82.109.176	9.9(1)	7.9(1)	4.27 GB	Not Configured	Single Context
FW-4-ASA	9.6(1)	7.6(1)	3.97 GB	Not Configured	Multi-Context Admin

[Continue](#) [View not upgradable devices \(1\)](#)

Step 8

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

Software Image

9.6(2)

9.9(1.2) 3 Devices

9.9(1) 2 Devices

9.8(2) 2 Devices

9.8(1) 2 Devices

9.6(1) 1 Devices

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 than it already runs.

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 9

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 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.

Upgrade Multiple ASAs with Images from your own Repository

Procedure

- Step 1** (Optional) In the left pane, click **Security Devices**.
- Step 2** Click the **Devices** tab.
- Step 3** From the filtered list of devices, select the devices you want to upgrade.
- Step 4** In the **Device Actions** pane, click **Upgrade**.
- Step 5** In step 1, click **Specify Image URL**, enter the URL to the ASA image you want to upgrade to in the **Software Image URL** field, and click **Continue**. See [Custom URL Upgrade](#) 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 [Custom URL Upgrade](#) for URL syntax information.

1 ASA Software Image

Please ensure the following before proceeding with the upgrade:

- DNS is configured properly on each device. For details, reference [Configure DNS on ASA](#)
- Each device has HTTPS connectivity to the internet in order to download the upgrade image.

Image Source

☐ Use CDO Image Repository

☒ Specify Image URL

Software Image URL:

You can specify a custom image URL if your device does not have outbound access to the internet or you need an image that CDO does not currently provide. This URL must be accessible from your device.

NAME	SOFTWARE	ASDM VERSION	FREE SPACE	FAILOVER MODE	CONTEXT MODE
10.82.109.176	9.9(1)	7.9(1)	4.27 GB	Not Configured	Single Context
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

[Continue](#)

- Step 6** In step 2, click **Specify Image URL**, enter the URL to the ASDM image you want to upgrade to in the **Software Image URL** field, and click **Continue**.

- Step 7** 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.
- 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 9** 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 10** (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 11** 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 12** 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 **Security Devices** 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 **Security Devices** 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** 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**.
- Step 5** 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 [Custom URL Upgrade](#) 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 6 Click **Perform Upgrade** when you are ready.

Step 7 (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 **Security Devices** 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 **Security Devices** 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 **Security Devices** 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 [ASA and ASDM Upgrade Prerequisites](#) 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 **Inventory**.
- Step 2** In the left pane, click **Security Devices**.

- Step 3** Click the **Devices** tab.
- Step 4** Select the device you want to upgrade.
- Step 5** In the **Device Actions** pane, click **Upgrade**.

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

Device Details	
Location	
Model	ASAv (V01)
Serial	
Chassis Serial	
Software Version	9.12(1)
ASDM Version	7.12(2)
Context Mode	Single Context
Firewall Mode	routed
Uptime	150 days 19 hours?
Failover Mode	Active/Standby
This Host	Primary - Active
Other Host	Secondary - Failed
SDC	

- Step 6** 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 [Custom URL Upgrade](#) 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 ]]
```

The **type** can be one of these keywords: **ap** (ASCII passive mode), **an** (ASCII normal mode), **ip** (Default 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 ]]
```

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.

