



Managing Software and Configurations

This chapter describes how to manage the ASA software and configurations and includes the following sections:

- [Upgrading the Software, page 84-1](#)
- [Managing Files, page 84-14](#)
- [Configuring the Images and Startup Configuration to Use, page 84-19](#)
- [Backing Up and Restoring Configurations or Other Files, page 84-20](#)
- [Saving the Running Configuration to a TFTP Server, page 84-27](#)
- [Scheduling a System Restart, page 84-27](#)
- [Downgrading Your Software, page 84-28](#)
- [Configuring Auto Update, page 84-30](#)

Upgrading the Software

This section describes how to upgrade to the latest version and includes the following topics:

- [Upgrade Path and Migrations, page 84-1](#)
- [Viewing Your Current Version, page 84-3](#)
- [Downloading the Software from Cisco.com, page 84-3](#)
- [Upgrading a Standalone Unit, page 84-3](#)
- [Upgrading a Failover Pair or ASA Cluster, page 84-8](#)



Note

For CLI procedures, see the ASA documentation.

Upgrade Path and Migrations



- If you are upgrading from a pre-8.3 release:
 - See the [Cisco ASA 5500 Migration Guide to Version 8.3 and Later](#) for important information about migrating your configuration.

- You cannot upgrade directly to 9.0 or later. You must first upgrade to Version 8.3 or 8.4 for a successful migration.
- When upgrading to Version 9.0, because of ACL migration, you cannot later perform a downgrade; be sure to back up your configuration file in case you want to downgrade. See the ACL migration section in the release notes for more information.
- Software Version Requirements for Zero Downtime Upgrading:

The units in a failover configuration or ASA cluster should have the same major (first number) and minor (second number) software version. However, you do not need to maintain version parity on the units during the upgrade process; you can have different versions on the software running on each unit and still maintain failover support. To ensure long-term compatibility and stability, we recommend upgrading all units to the same version as soon as possible.

Table 1-1 shows the supported scenarios for performing zero-downtime upgrades.

Table 84-1 Zero-Downtime Upgrade Support

Type of Upgrade	Support
Maintenance Release	<p>You can upgrade from any maintenance release to any other maintenance release within a minor release.</p> <p>For example, you can upgrade from 8.4(1) to 8.4(6) without first installing the maintenance releases in between.</p>
Minor Release	<p>You can upgrade from a minor release to the next minor release. You cannot skip a minor release.</p> <p>For example, you can upgrade from 8.2 to 8.3. Upgrading from 8.2 directly to 8.4 is not supported for zero-downtime upgrades; you must first upgrade to 8.3. For models that are not supported on a minor release, you can skip the minor release; for example, for the ASA 5585-X, you can upgrade from 8.2 to 8.4 (the model is not supported on 8.3).</p> <div>  <p>Note Zero-downtime upgrades are possible, even when feature configuration is migrated, for example, from 8.2 to 8.3.</p> </div>
Major Release	<p>You can upgrade from the last minor release of the previous version to the next major release.</p> <p>For example, you can upgrade from 8.6 to 9.0, assuming that 8.6 is the last minor version in the 8.x release series for your model. Upgrading from 8.6 directly to 9.1 is not supported for zero-downtime upgrades; you must first upgrade to 9.0. For models that are not supported on a minor release, you can skip the minor release; for example, for the ASA 5585-X, you can upgrade from 8.4 to 9.0 (the model is not supported on 8.5 or 8.6).</p> <div>  <p>Note Zero-downtime upgrades are possible, even when feature configuration is migrated, for example, from 8.4 to 9.0.</p> </div>

Viewing Your Current Version

The software version appears on the ASDM home page; view the home page to verify the software version of your ASA.

Downloading the Software from Cisco.com

If you are using the ASDM Upgrade Wizard, you do not have to pre-download the software. If you are manually upgrading, for example for a failover upgrade, download the images to your local computer.

If you have a Cisco.com login, you can obtain the OS and ASDM images from the following website:

<http://www.cisco.com/cisco/software/navigator.html?mdfid=279513386>

Upgrading a Standalone Unit



Note

This section describes how to install the ASDM and operating system (OS) images. If the ASA is running Version 8.0 or later, then you can upgrade to the latest version of ASDM (and disconnect and reconnect to start running it) before upgrading the OS. The exception is for ASA versions that are not supported by the latest ASDM version; for example, ASA 8.5. In that case, follow the instructions for pre-8.0 versions (ASDM 5.2 and earlier).

If the ASA is running a version earlier than 8.0, then use the already installed version of ASDM to upgrade both the OS and ASDM to the latest versions, and then reload.

- [Upgrading from Your Local Computer \(ASDM 6.0 or Later\)](#), page 84-3
- [Upgrading Using the Cisco.com Wizard \(ASDM 6.3 or Later\)](#), page 84-5
- [Upgrading Using the Cisco.com Wizard \(ASDM 6.0 Through ASDM 6.2\)](#), page 84-6
- [Upgrading from Your Local Computer \(ASDM 5.2 or Earlier\)](#), page 84-7

Upgrading from Your Local Computer (ASDM 6.0 or Later)

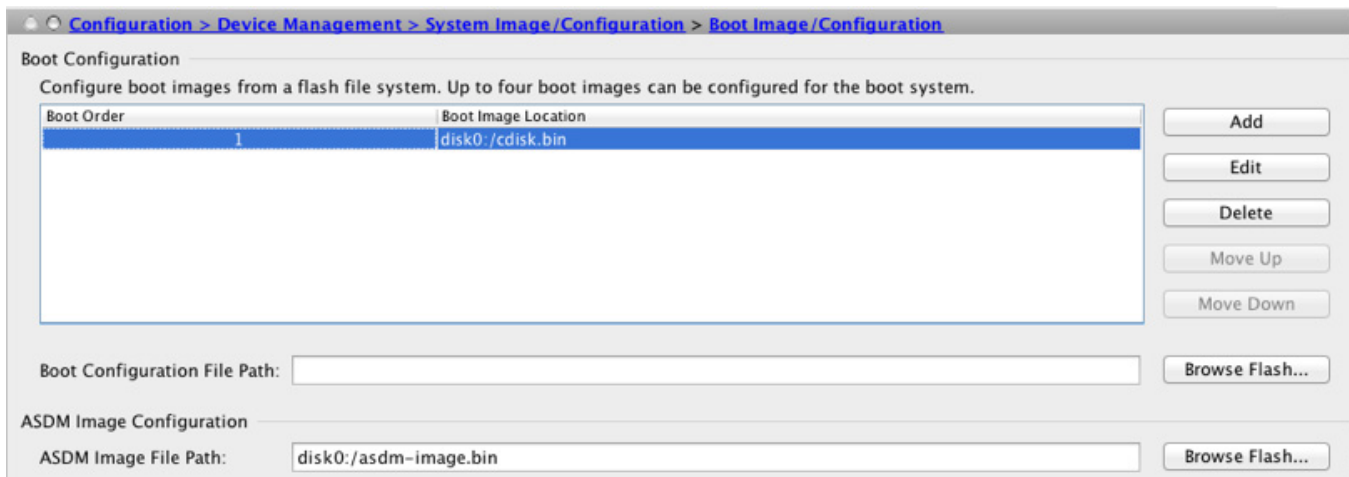
The Upgrade Software from Local Computer tool lets you upload an image file from your computer to the flash file system to upgrade the ASA.

To upgrade software from your computer, perform the following steps:

- Step 1** (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.
- Step 2** In the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**. The Upgrade Software dialog box appears.



- Step 3** From the Image to Upload drop-down list, choose **ASDM**.
- Step 4** In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.
- Step 5** In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.
- Step 6** Click **Upload Image**. The uploading process might take a few minutes.
- Step 7** Repeat [Step 2](#) through [Step 6](#), choosing **ASA** from the Image to Upload drop-down list. You can also use this procedure to upload other file types.
- Step 8** Configure the ASA to use the new images.
 - a. Choose **Configuration > Device Management > System/Image Configuration > Boot Image/Configuration**.



- b. In the Boot Configuration table, click **Add** to add the new image (if you have fewer than four images listed); or you can choose an existing image and click **Edit** to change it to the new one.
If you do not specify an image, the ASA searches the internal flash memory for the first valid image to boot; we recommend booting from a specific image.
- c. Click **Browse Flash**, choose the OS image, and click **OK**.
- d. Click **OK** to return to the Boot Image/Configuration pane.
- e. Make sure the new image is the first image in the table by using the **Move Up** button as needed.

- f. In the ASDM Image Configuration area, click **Browse Flash**, choose the ASDM image, and click **OK**.
- g. Click **Apply**.

Step 9 Choose **File > Save Running Configuration to Flash** to save your configuration changes.

Step 10 Choose **Tools > System Reload** to reload the ASA.

A new window appears that asks you to verify the details of the reload. Click the **Save the running configuration at the time of reload** radio button, choose a time to reload (for example, **Now**), and click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 11 After the ASA reloads, restart ASDM.

Upgrading Using the Cisco.com Wizard (ASDM 6.3 or Later)

The Upgrade Software from Cisco.com Wizard lets you automatically upgrade the ASDM and ASA to more current versions.

In this wizard, you can do the following:

- Choose an ASA image file and/or ASDM image file to upgrade.



Note

ASDM downloads the latest image version, which includes the build number. For example, if you are downloading 8.4(2), the download might be 8.4(2.8). This behavior is expected, so you may proceed with the planned upgrade.

- Review the upgrade changes that you have made.
- Download the image or images and install them.
- Review the status of the installation.
- If the installation completed successfully, restart the ASA to save the configuration and complete the upgrade.

Detailed Steps

Step 1 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 2 Choose **Tools > Check for ASA/ASDM Updates**.

In multiple context mode, access this menu from the System.

The Cisco.com Authentication dialog box appears.

Step 3 Enter your assigned Cisco.com username and the Cisco.com password, and then click **Login**.

The Cisco.com Upgrade Wizard appears.



Note

If there are no upgrade available, a dialog box appears. Click **OK** to exit the wizard.

- Step 4** Click **Next** to display the Select Software screen.
The current ASA version and ASDM version appear.
- Step 5** To upgrade the ASA version and ASDM version, perform the following steps:
- In the ASA area, check the **Upgrade to** check box, and then choose an ASA version to which you want to upgrade from the drop-down list.
 - In the ASDM area, check the **Upgrade to** check box, and then choose an ASDM version to which you want to upgrade from the drop-down list.
- Step 6** Click **Next** to display the Review Changes screen.
- Step 7** Verify the following items:
- The ASA image file and/or ASDM image file that you have downloaded are the correct ones.
 - The ASA image file and/or ASDM image file that you want to upload are the correct ones.
 - The correct ASA boot image has been selected.
- Step 8** Click **Next** to start the upgrade installation.
You can then view the status of the upgrade installation as it progresses.
The Results screen appears, which provides additional details, such as the upgrade installation status (success or failure).
During the upgrade process from Version 8.2(1) to Version 8.3(1), the following files are automatically saved to flash memory:
- The startup configuration
 - The per-context configuration
 - The bootup error log, which includes any migration messages
- If there is insufficient memory to save the configuration files, an error message appears on the console of the ASA and is saved in the bootup error log file. All previously saved configuration files are also removed.
- Step 9** If the upgrade installation succeeded, for the upgrade versions to take effect, check the **Save configuration and reload device now** check box to restart the ASA, and restart ASDM.
- Step 10** Click **Finish** to exit the wizard and save the configuration changes that you have made.



Note To upgrade to the next higher version, if any, you must restart the wizard.

Upgrading Using the Cisco.com Wizard (ASDM 6.0 Through ASDM 6.2)

Detailed Steps

- Step 1** (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.
- Step 2** From the Tools menu, choose **Tools > Upgrade Software from Cisco.com**.
In multiple context mode, access this menu from the System.
The Upgrade Software from Cisco.com Wizard appears.

- Step 3** Click **Next**.
The Authentication screen appears.
- Step 4** Enter your Cisco.com username and password, and click **Next**.
The Image Selection screen appears.
- Step 5** Check the **Upgrade the ASA version** check box and the **Upgrade the ASDM version** check box to specify the most current images to which you want to upgrade, and click **Next**.
The Selected Images screen appears.
- Step 6** Verify that the image file you have selected is the correct one, and then click **Next** to start the upgrade.
The wizard indicates that the upgrade will take a few minutes. You can then view the status of the upgrade as it progresses.
The Results screen appears. This screen provides additional details, such as whether the upgrade failed or whether you want to save the configuration and reload the ASA.
If you upgraded the ASA version and the upgrade succeeded, an option to save the configuration and reload the ASA appears.
- Step 7** Click **Yes**.
For the upgrade versions to take effect, you must save the configuration, reload the ASA, and restart ASDM.
- Step 8** Click **Finish** to exit the wizard when the upgrade is finished.
- Step 9** After the ASA reloads, restart ASDM.
-

Upgrading from Your Local Computer (ASDM 5.2 or Earlier)

Detailed Steps

- Step 1** (If there is a configuration migration) In ASDM, back up your existing configuration. For example, choose **File > Show Running Configuration in New Window** to open the configuration as an HTML page. You can also use one of the File > Save Running Configuration options.
- Step 2** Choose **Tools > Upgrade Software**.
- Step 3** From the Image to Upload drop-down list, choose **ASDM**.
- Step 4** Click **Browse Local Files**, and browse to the ASDM image you downloaded from Cisco.com.
- Step 5** Click **Browse Flash** to determine where to install the new ASDM image.
The Browse Flash dialog box appears. Choose the new location, and click **OK**. If you do not have room for both the current image and the new image, you can install over the current image.
- Step 6** Click **Upload Image**.
Wait for the image to upload. An information window appears that indicates a successful upload.
- Step 7** Repeat [Step 2](#) through [Step 6](#), choosing **ASA** from the Image to Upload drop-down list.
- Step 8** Click **Close** to exit the Upgrade Software dialog box.
- Step 9** Configure the ASA to use the new images.
a. Choose **Configuration > Properties > Device Administration > Boot Image/Configuration**.

- b. In the Boot Configuration table, click **Add** to add the new image (if you have fewer than four images listed); or you can choose an existing image and click **Edit** to change it to the new one.
If you do not specify an image, the ASA searches the internal flash memory for the first valid image to boot; we recommend booting from a specific image.
- c. Click **Browse Flash**, choose the OS image, and click **OK**.
- d. Click **OK** to return to the Boot Image/Configuration pane.
- e. Make sure the new image is the first image in the table by using the **Move Up** button as needed.
- f. In the ASDM Image Configuration area, click **Browse Flash**, choose the ASDM image, and click **OK**.
- g. Click **Apply**.

Step 10 Choose **File > Save Running Configuration to Flash** to save your configuration changes.

Step 11 Choose **Tools > System Reload** to reload the ASA.

A new window appears that asks you to verify the details of the reload. Click the **Save the running configuration at the time of reload** radio button, choose a time to reload (for example, **Now**), and click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 12 After the ASA reloads, restart ASDM.

Upgrading a Failover Pair or ASA Cluster

- [Upgrading an Active/Standby Failover Pair, page 84-8](#)
- [Upgrading an ASA Cluster, page 84-12](#)

Upgrading an Active/Standby Failover Pair

To upgrade the Active/Standby failover pair, perform the following steps.

Detailed Steps

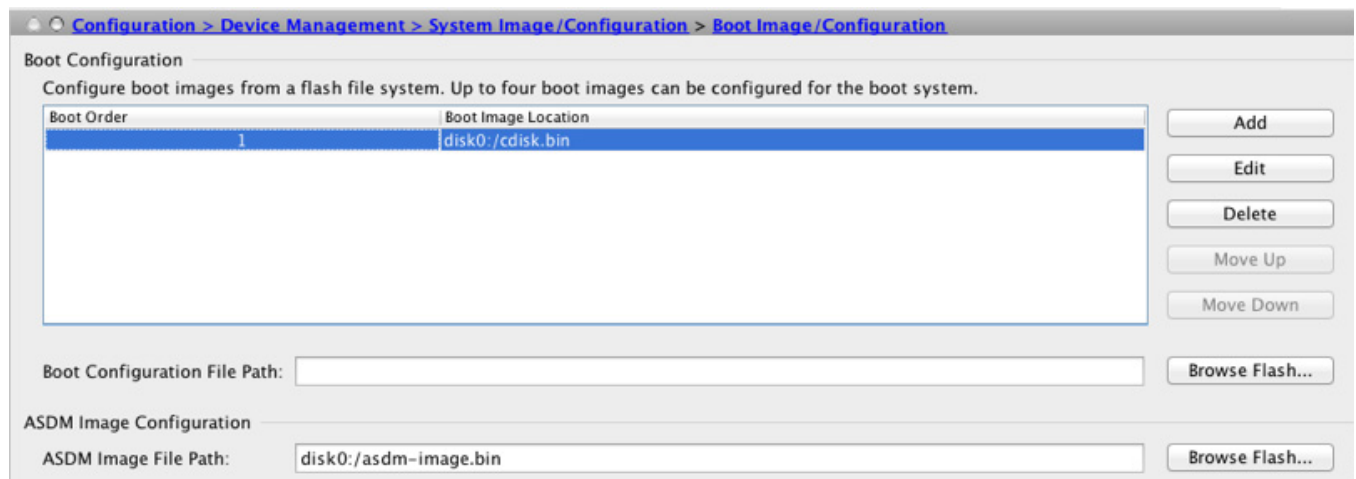
Step 1 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 2 On the active unit, in the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**.

The Upgrade Software dialog box appears.



- Step 3** From the Image to Upload drop-down list, choose **ASDM**.
- Step 4** In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.
- Step 5** In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.
- Step 6** Click **Upload Image**. The uploading process might take a few minutes.
- Step 7** Repeat [Step 2](#) through [Step 6](#), choosing **ASA** from the Image to Upload drop-down list.
- Step 8** Configure the ASA to use the new images.
- Choose **Configuration > Device Management > System/Image Configuration > Boot Image/Configuration**.



- In the Boot Configuration table, click **Add** to add the new image (if you have fewer than four images listed); or you can choose an existing image and click **Edit** to change it to the new one.
If you do not specify an image, the ASA searches the internal flash memory for the first valid image to boot; we recommend booting from a specific image.
- Click **Browse Flash**, choose the OS image, and click **OK**.
- Click **OK** to return to the Boot Image/Configuration pane.
- Make sure the new image is the first image in the table by using the **Move Up** button as needed.
- In the ASDM Image Configuration area, click **Browse Flash**, choose the ASDM image, and click **OK**.

g. Click **Apply**.

Step 9 Choose **File > Save Running Configuration to Flash** to save your configuration changes.

Step 10 Connect ASDM to the *standby* unit, and upload the ASA and ASDM software according to [Step 2](#) through [Step 7](#), using the same file locations you used on the active unit.

Step 11 Choose **Tools > System Reload** to reload the standby ASA.

A new window appears that asks you to verify the details of the reload. Click the **Save the running configuration at the time of reload** radio button, choose a time to reload (for example, **Now**), and click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 12 After the standby ASA reloads, restart ASDM and connect to the standby unit to make sure it is running.

Step 13 Connect ASDM to the *active* unit again.

Step 14 Force the active unit to fail over to the standby unit by choosing **Monitoring > Properties > Failover > Status**, and clicking **Make Standby**.

Step 15 Choose **Tools > System Reload** to reload the (formerly) active ASA.

A new window appears that asks you to verify the details of the reload. Click the **Save the running configuration at the time of reload** radio button, choose a time to reload (for example, **Now**), and click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

After the ASA comes up, it will now be the standby unit.

Upgrading an Active/Active Failover Pair

To upgrade two units in an Active/Active failover configuration, perform the following steps.

Requirements

Perform these steps in the system execution space.

Detailed Steps

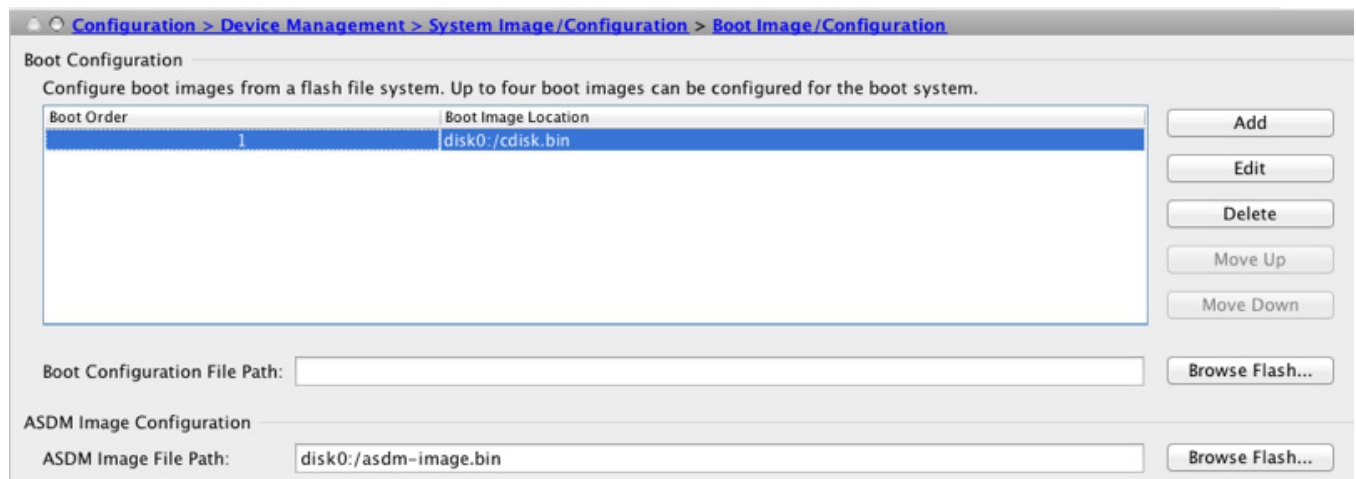
Step 1 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 2 On the primary unit, in the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**.

The Upgrade Software dialog box appears.



- Step 3** From the Image to Upload drop-down list, choose **ASDM**.
- Step 4** In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.
- Step 5** In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.
- Step 6** Click **Upload Image**. The uploading process might take a few minutes.
- Step 7** Repeat [Step 2](#) through [Step 6](#), choosing **ASA** from the Image to Upload drop-down list.
- Step 8** Configure the ASA to use the new images.
- Choose **Configuration > Device Management > System/Image Configuration > Boot Image/Configuration**.



- In the Boot Configuration table, click **Add** to add the new image (if you have fewer than four images listed); or you can choose an existing image and click **Edit** to change it to the new one.
If you do not specify an image, the ASA searches the internal flash memory for the first valid image to boot; we recommend booting from a specific image.
- Click **Browse Flash**, choose the OS image, and click **OK**.
- Click **OK** to return to the Boot Image/Configuration pane.
- Make sure the new image is the first image in the table by using the **Move Up** button as needed.
- In the ASDM Image Configuration area, click **Browse Flash**, choose the ASDM image, and click **OK**.

g. Click **Apply**.

Step 9 Choose **File > Save Running Configuration to Flash** to save your configuration changes.

Step 10 Make both failover groups active on the primary unit by choosing **Monitoring > Failover > Failover Group #**, where # is the number of the failover group you want to move to the primary unit, and clicking **Make Active**.

Step 11 Connect ASDM to the *secondary* unit, and upload the ASA and ASDM software according to [Step 2](#) through [Step 7](#), using the same file locations you used on the active unit.

Step 12 Choose **Tools > System Reload** to reload the secondary ASA.

A new window appears that asks you to verify the details of the reload. Click the **Save the running configuration at the time of reload** radio button, choose a time to reload (for example, **Now**), and click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

Step 13 Connect ASDM to the *primary* unit, and check when the secondary unit reloads by choosing **Monitoring > Failover > System**.

Step 14 After the secondary unit comes up, force the primary unit to fail over to the secondary unit by choosing **Monitoring > Properties > Failover > System**, and clicking **Make Standby**.

Step 15 Choose **Tools > System Reload** to reload the (formerly) active ASA.

A new window appears that asks you to verify the details of the reload. Click the **Save the running configuration at the time of reload** radio button, choose a time to reload (for example, **Now**), and click **Schedule Reload**.

Once the reload is in progress, a Reload Status window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with Preempt Enabled, you can return them to active status on their designated units using the **Monitoring > Failover > Failover Group #** pane.

Upgrading an ASA Cluster

To upgrade all units in an ASA cluster, perform the following steps on the master unit. For multiple context mode, perform these steps in the system execution space.

Detailed Steps

Step 1 Launch ASDM on the master unit.

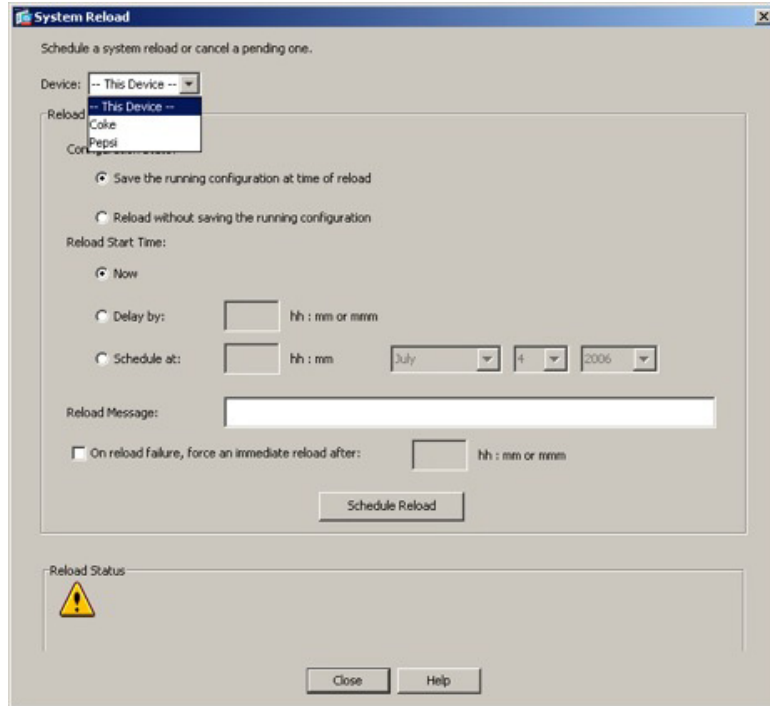
Step 2 (If there is a configuration migration) In ASDM, back up your existing configuration using the **Tools > Backup Configurations** tool.

Step 3 In the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**. The Upgrade Software from Local Computer dialog box appears.

Step 4 Click the **All devices in the cluster** radio button.



- Step 5** From the Image to Upload drop-down list, choose the new image file.
- Step 6** In the Local File Path field, enter the local path to the file on your computer or click **Browse Local Files** to find the file on your PC.
- Step 7** In the Flash File System Path field, enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.
- Step 8** Click **Upload Image**. The uploading process might take a few minutes; make sure you wait until it is finished.
- Step 9** Choose **Tools > System Reload**.
The System Reload dialog box appears.
- Step 10** Reload each slave unit one at a time by choosing a slave unit name in the Device drop-down list, and then clicking **Schedule Reload** to reload the unit now.



To avoid connection loss, wait for each unit to come back up before reloading the next unit. To view when a unit rejoins the cluster, see the Monitoring > ASA Cluster > Cluster Summary pane.

- Step 11** After all slave units have reloaded, reload the master unit from the System Reload dialog box by choosing **--This Device--** from the Device drop-down list.
- A new election takes place for a new master unit. When the former master unit rejoins the cluster, it will be a slave.
- Step 12** Quit and restart ASDM; you will reconnect to the new master unit.
-

Managing Files

ASDM provides a set of file management tools to help you perform basic file management tasks. The File Management tool lets you view, move, copy, and delete files stored in flash memory, transfer files, and to manage files on remote storage devices (mount points).

**Note**

In multiple context mode, this tool is only available in the system security context.

- [Accessing the File Management Tool, page 84-14](#)
- [Managing Mount Points, page 84-15](#)
- [Transferring Files, page 84-17](#)

Accessing the File Management Tool

To use the file management tools, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > File Management**.
- The File Management dialog box appears.
- The Folders pane displays the available folders on disk.
 - Flash Space shows the total amount of flash memory and how much memory is available.
 - The Files area displays the following information about files in the selected folder:
 - Path
 - Filename
 - Size (bytes)
 - Time Modified
 - Status, which indicates whether a selected file is designated as a boot configuration file, boot image file, ASDM image file, SVC image file, CSD image file, or APCF image file.
- Step 2** Click **View** to display the selected file in your browser.
- Step 3** Click **Cut** to cut the selected file for pasting to another directory.
- Step 4** Click **Copy** to copy the selected file for pasting to another directory.
- Step 5** Click **Paste** to paste the copied file to the selected destination.
- Step 6** Click **Delete** to remove the selected file from flash memory.

- Step 7** Click **Rename** to rename a file.
- Step 8** Click **New Directory** to create a new directory for storing files.
- Step 9** Click **File Transfer** to open the File Transfer dialog box. See the [“Transferring Files” section on page 84-17](#) for more information.
- Step 10** Click **Mount Points** to open the Manage Mount Points dialog box. See the [“Managing Mount Points” section on page 84-15](#) for more information.
-

Managing Mount Points

This feature lets you configure remote storage (mount points) for network file systems using a CIFS or FTP connection. The dialog box lists the mount-point name, connection type, server name or IP address, and the enabled setting (yes or no). You can add, edit, or delete mount points. See the [“Adding or Editing a CIFS/FTP Mount Point” section on page 84-15](#) for more information. You can access a CIFS mount point after it has been created. For more information, see [Accessing a CIFS Mount Point, page 84-16](#).

This section includes the following topics:

- [Adding or Editing a CIFS/FTP Mount Point, page 84-15](#)
- [Accessing a CIFS Mount Point, page 84-16](#)

Adding or Editing a CIFS/FTP Mount Point

To add a CIFS mount point, perform the following steps:

-
- Step 1** Click **Add**, and then choose **CIFS Mount Point**.
The Add CIFS Mount Point dialog box appears.
The Enable mount point check box is automatically checked, which is the default setting.
- Step 2** Enter the mount-point name, server name or IP address, and share name in the applicable fields.
- Step 3** In the Authentication section, enter the NT domain, username and password, and then confirm the password.
- Step 4** Click **OK**.
-

To add an FTP mount point, perform the following steps:

-
- Step 1** Click **Add**, and then choose **FTP Mount Point**.
The Add FTP Mount Point dialog box appears.
The Enable mount point check box is automatically checked, which is the default setting.
- Step 2** Enter the mount-point name and the server name or IP address in the applicable fields.
- Step 3** In the FTP Mount Options area, click the **Active Mode** or **Passive Mode** option.
- Step 4** Enter the path to mount the remote storage.
- Step 5** In the Authentication area, enter the NT domain, username and password, and then confirm the password.

Step 6 Click **OK**.

To edit a CIFS mount point, perform the following steps:

Step 1 Choose the CIFS mount-point you want to modify, and click **Edit**.

The Edit CIFS Mount Point dialog box appears.



Note You cannot change the CIFS mount-point name.

Step 2 Make the changes to the remaining settings, and click **OK** when you are done.

To edit an FTP mount point, perform the following steps:

Step 1 Choose the FTP mount-point you want to modify, and click **Edit**.

The Edit FTP Mount Point dialog box appears.



Note You cannot change the FTP mount-point name.

Step 2 Make the changes to the remaining settings, and click **OK** when you are done.

Accessing a CIFS Mount Point

To access a CIFS mount point after it has been created, perform the following steps:

Step 1 Start the ASA CLI.

Step 2 Create the mount by entering the **mount** *name of mount* **type cifs** command.

Step 3 Enter the **show run mount** command.

The following output appears:



Note In this example, win2003 is the name of the mount.

```
server kmmwin2003
share sharefolder
username webvpnuser2
password *****
status enable
```

Step 4 Enter the **dir** command to list all enabled mounts as subdirectories, which is similar to mounting a drive on the Windows PC. For example, in the following output, FTP2003:, FTPLINUX:, and win2K: are configured mounts.

The following is sample output from the **dir** command:


```

FTP2003: Directory or file name
FTPLINUX: Directory or file name
WIN2003: Directory or file name
all-filesystems List files on all filesystems
disk0: Directory or file name
disk1: Directory or file name
flash: Directory or file name
system: Directory or file name
win2K: Directory or file name

```

Step 5 Enter the **dir** command for that mount (for example, **dir WIN2003**), and copy files to and from flash (disk0:) to any of the listed mounts.

The following is sample output from the **dir WIN2003** command.

```

Directory of WIN2003:/
---- 14920928 08:33:36 Apr 03 2009 1_5_0_01-windows-i586-p.exe
---- 33 11:27:16 Jun 07 2007 AArenameIE70
---- 28213021 15:15:22 Apr 03 2009 atest2(3).bin
---- 61946730 12:09:40 Mar 17 2009 atest2.bin
---- 5398366 14:52:10 Jul 28 2008 atest222.bin
---- 2587728 10:07:44 Dec 06 2005 cCITRIXICA32t.exe
---- 1499578 15:26:50 Dec 02 2005 ccore.exe
---- 61946728 11:40:36 Dec 09 2005 CIFSTESTT.bin
---- 2828 13:46:04 May 11 2009 ClientCert.pfx
d--- 16384 14:48:28 Mar 20 2007 cookiefolder
---- 4399 15:58:46 Jan 06 2006 Cookies.plist
---- 2781710 12:35:00 Dec 12 2006 coreftplite1.3.exe
---- 0 10:22:52 Jul 13 2007 coreftplite1.3.exe.download
---- 245760 15:13:38 Dec 21 2005 Dbgview.exe
---- 1408249 11:01:34 Dec 08 2005 expect-5.21r1b1-setup.exe
d--- 16384 14:49:14 Jul 28 2008 folder157
---- 101 09:33:48 Dec 12 2005 FxSasser.log
---- 2307104 09:54:12 Dec 12 2005 ica32t.exe
---- 8732552 10:14:32 Apr 29 2009 iclientSetup_IFen_flex51.exe
d--- 16384 08:32:46 Apr 03 2009 IE8withVistaTitan
---- 15955208 08:34:18 Aug 14 2007 j2re.exe
---- 16781620 13:38:22 Jul 23 2008 jre-1_5_0_06-windows-i586-p.exe
<--- More --->

```

Transferring Files

The File Transfer tool lets you transfer files from either a local or remote location. You can transfer a local file on your computer or a flash file system to and from the ASA. You can transfer a remote file to and from the ASA using HTTP, HTTPS, TFTP, FTP, or SMB.



Note

For the IPS SSP software module, before you download the IPS software to disk0, make sure at least 50% of the flash memory is free. When you install IPS, IPS reserves 50% of the internal flash memory for its file system.

- [Transferring Files Between Local PC and Flash, page 84-18](#)
- [Transferring Files Between Remote Server and Flash, page 84-18](#)


Transferring Files Between Local PC and Flash

To transfer files between your local computer and a flash file system, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > File Management**.
The File Management dialog box appears.
- Step 2** Click the down arrow next to **File Transfer**, and then click **Between Local PC and Flash**.
The File Transfer dialog box appears.
- Step 3** Select and *drag* the file(s) from either your local computer or the flash file system that you want to upload or download to the desired location. Alternatively, select the file(s) from either your local computer or the flash file system that you want to upload or download, and click the right arrow or left arrow to transfer the file(s) to the desired location.
- Step 4** Click **Close** when you are done.
-

Transferring Files Between Remote Server and Flash

To transfer files between a remote server and a flash file system, perform the following steps:

-
- Step 1** In the main ASDM application window, choose **Tools > File Management**.
The File Management dialog box appears.
- Step 2** Click the down arrow from the File Transfer drop-down list, and then click **Between Remote Server and Flash**.
The File Transfer dialog box appears.
- Step 3** To transfer a file from a remote server, click the **Remote server** option.
- Step 4** Define the source file to be transferred.
- Choose the path to the location of the file, including the IP address of the server.
- 
- Note** File transfer supports IPv4 and IPv6 addresses.
- Enter the type (if the path is FTP) or the port number (if the path is HTTP or HTTPS) of the remote server. Valid FTP types are the following:
 - ap—ASCII files in passive mode
 - an—ASCII files in non-passive mode
 - ip—Binary image files in passive mode
 - in—Binary image files in non-passive mode
- Step 5** To transfer the file from the flash file system, click the **Flash file system** option.
- Step 6** Enter the path to the location of the file or click **Browse Flash** to find the file location.
- Step 7** In addition, you can copy a file from your startup configuration, running configuration, or an SMB file system through the CLI. For instructions about using the **copy** command, see the CLI configuration guide.

- Step 8** Define the destination of the file to be transferred.
- To transfer the file to the flash file system, choose the **Flash file system** option.
 - Enter the path to the location of the file or click **Browse Flash** to find the file location.
- Step 9** To transfer a file to a remote server, choose the **Remote server** option.
- Enter the path to the location of the file.
 - For FTP transfers, enter the type. Valid types are the following:
 - ap—ASCII files in passive mode
 - an—ASCII files in non-passive mode
 - ip—Binary image files in passive mode
 - in—Binary image files in non-passive mode
- Step 10** Click **Transfer** to start the file transfer.
- The Enter Username and Password dialog box appears.
- Step 11** Enter the username, password, and domain (if required) for the remote server.
- Step 12** Click **OK** to continue the file transfer.
- The file transfer process might take a few minutes; make sure that you wait until it is finished.
- Step 13** Click **Close** when the file transfer is finished.
-

Configuring the Images and Startup Configuration to Use

By default, the ASA boots the first application image that it finds in internal flash memory. It also boots the first ASDM image it finds in internal flash memory, or if one does not exist in this location, then in external flash memory. If you have more than one image, you should specify the image that you want to boot. For the ASDM image, if you do not specify the image to boot, even if you have only one image installed, then the ASA defines the image in the running configuration. To avoid problems with Auto Update (if configured), and to avoid the image search at each startup, you should specify the ASDM image that you want to boot in the startup configuration.

Choose **Configuration > Device Management > System Image/Configuration > Boot Image/Configuration**.

You can specify up to four local binary image files for use as the startup image, and one image located on a TFTP server for the device to boot from. If you specify an image located on a TFTP server, it must be first in the list. If the device cannot reach the TFTP server to load the image, it tries to load the next image file in the list located in flash.

If you do not specify any boot variable, the first valid image on internal flash will be chosen to boot the system. The Boot Image/Configuration pane includes the following fields:

- **Boot Order**—Displays the order in which binary image files will be used to boot.
- **Boot Image Location**—Displays the physical location and path of the boot file.
- **Boot Configuration File Path**—Displays the location of the configuration file.
- **Add**—Lets you add a flash or TFTP boot image entry to be used in the boot process. For more information, see the [“Adding a Boot Image” section on page 84-20](#).
- **Edit**—Lets you edit a flash or TFTP boot image entry.

- Delete—Deletes the selected flash or TFTP boot image entry.
- Move Up—Moves the selected flash or TFTP boot image entry up in the boot order.
- Move Down—Moves the selected flash or TFTP boot image entry down in the boot order.
- Browse Flash—Lets you specify the location of a boot image or configuration file.
- ASDM Image File Path—Displays the location of the configuration file to use at startup.

Adding a Boot Image

To add a boot image entry to the boot order list, click **Add** in the Boot Image/Configuration pane.

You can select a flash or TFTP image to add a boot image to the boot order list.

Either type the path of the image, or click **Browse Flash** to specify the image location. You must type the path of the image location if you are using TFTP.

- Flash Image—Select to add a boot image located in the flash file system.
 - Path—Specify the path of the boot image in the flash file system.
- TFTP Image—Select to add a boot image located on a TFTP server.
 - [Path]—Enter the path of the boot image file on the TFTP server, including the IP address of the server.
- OK—Accepts changes and returns to the previous pane.
- Cancel—Discards changes and returns to the previous pane.
- Help—Provides more information.

Backing Up and Restoring Configurations or Other Files

The Backup and Restore features options on the Tools menu let you back up and restore the ASA running configuration, startup configuration, installed add-on images, and SSL VPN Client images and profiles.

The Backup Configurations screen on the ASDM lets you choose the file types to back up, compresses them into a single zip file, then transfer the zip file to the directory that you choose on your computer. Similarly, to restore files, you choose the source zip file on your computer and then choose the file types to be restored.



Note

These tools are only available for single context mode.

- [Backing Up Configurations, page 84-21](#)
- [Backing Up the Local CA Server, page 84-24](#)
- [Restoring Configurations, page 84-25](#)
- [Saving the Running Configuration to a TFTP Server, page 84-27](#)

Backing Up Configurations

This procedure explains how to back up configurations and images to a .zip file and transfer it to your local computer.

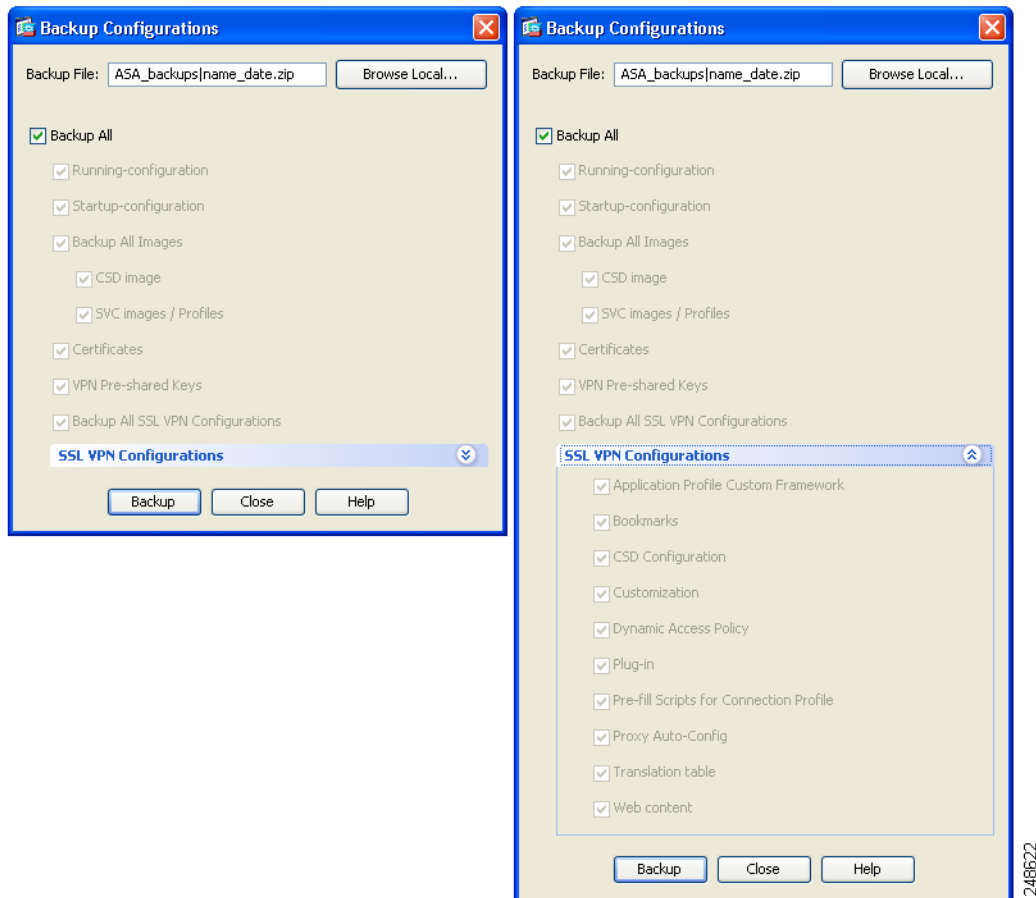


Caution

If you have set a master passphrase for the ASA, then you will need that master passphrase to restore the backup configuration that you create with this procedure. If you do not know the master passphrase for the ASA, see the [“Configuring the Master Passphrase”](#) section on page 14-5 to learn how to reset it before continuing with the backup.

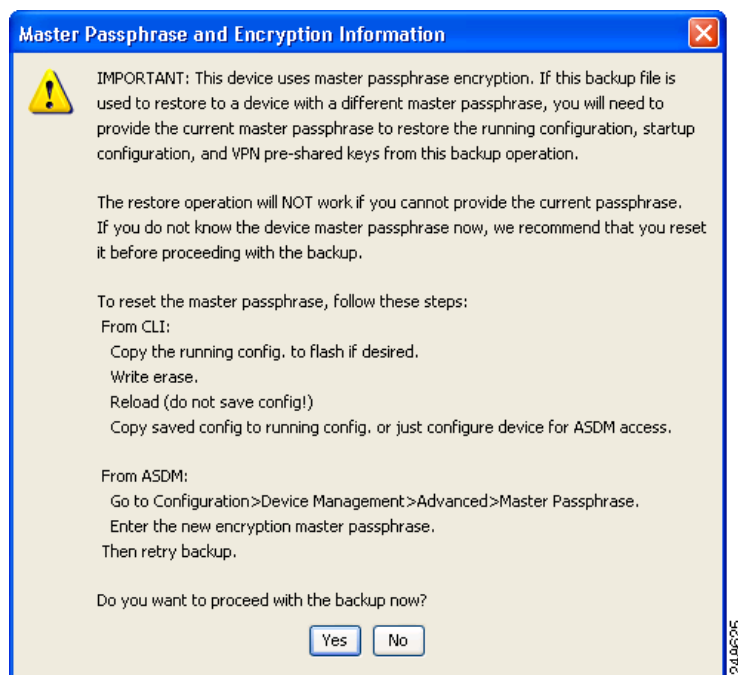
- Step 1** Create a folder on your computer to store backup files so they will be easy to find in case you need to restore them later.
- Step 2** Choose **Tools > Backup Configurations**.

The Backup Configurations dialog box appears. Click the down arrow in the **SSL VPN Configuration** area to view the backup options for SSL VPN configurations. By default, all configuration files are checked and will be backed up if they are available. If you want to back up all of the files in the list, go to Step 5.



- Step 3** Uncheck the **Backup All** check box if you want to select the configurations to back up.
- Step 4** Check the check box next to the option that you want to back up.

- Step 5** Click **Browse Local** to specify a directory and file name for the backup .zip file.
- Step 6** In the Select dialog box, choose the directory in which you want to store the backup file.
- Step 7** Click **Select**. The path appears in the Backup File field.
- Step 8** Enter the name of the destination backup file after the directory path. The backup file name must be between 3 and 232 characters long.
- Step 9** Click **Backup**. The backup proceeds immediately unless you are backing up certificates or the ASA is using a master passphrase.
- Step 10** If you have configured and enabled a master passphrase on your ASA, you receive a warning message with a suggestion to change the master passphrase, if you do not know it, before proceeding with the backup. Click **Yes** to proceed with the backup if you know the master passphrase. The backup proceeds immediately unless you are backing up identity certificates.



- Step 11** If you are backing up an identity certificate, you are asked to enter a separate passphrase to be used for encoding the certificates in PKCS12 format. You can enter a passphrase or skip this step.

**Note**

Identify certificates are backed up by this process; however, certificate authority certificates are not backed up. For instructions on backing up CA certificates, see [“Backing Up the Local CA Server” section on page 84-24](#).



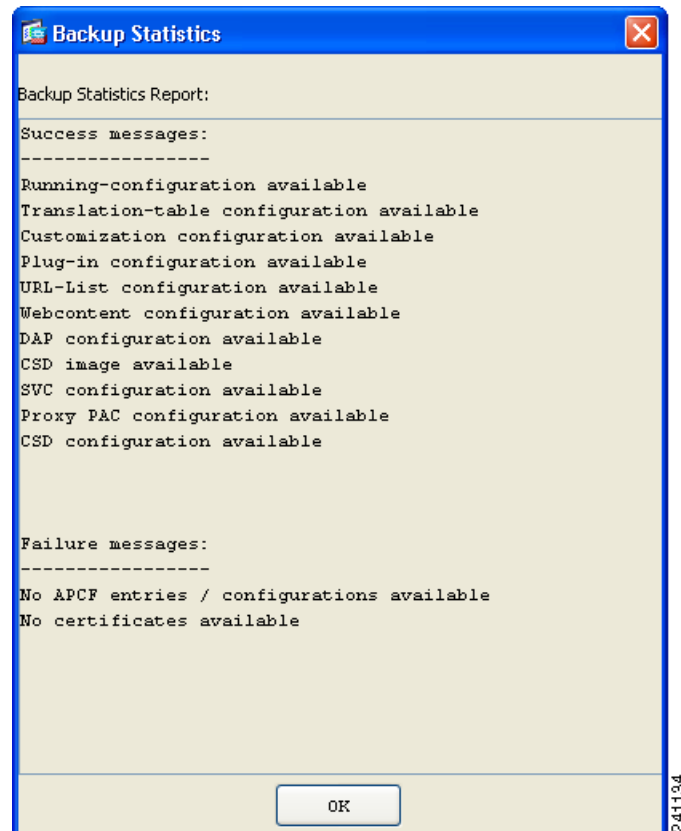
- To encrypt certificates, enter and confirm your certificate passphrase in the Certificate Passphrase dialog box and click **OK**. You will need to remember the password you enter in this dialog box when restoring the certificates.
- Clicking **Cancel** skips the step and does not back up certificates.

After clicking OK or cancel, the backup begins immediately.

Step 12 After the backup is complete, the status window closes and the Backup Statistics dialog box appears to provide success and failure messages.



Note Backup “failure messages” are most likely caused by the lack of an existing configuration for the types indicated.



Step 13 Click **OK** to close the Backup Statistics dialog box.

Backing Up the Local CA Server

When you do a ASDM backup, it does not include the local CA server database, so you are not backing up the CA certificates stored on the server. If you want to back up the local CA server, use this manual process with the ASA CLI:

Step 1 Enter the **show run crypto ca server** command.

```
crypto ca server
  keysize server 2048
  subject-name-default OU=aa,O=Cisco,ST=ca,
  issuer-name CN=xxx,OU=yyy,O=Cisco,L=Bxb,St=Mass
  smtp from-address abcd@cisco.com
  publish-crl inside 80
  publish-crl outside 80
```

Step 2 Use the **crypto ca import** command to import the local CA PKCS12 file to create the LOCAL-CA-SERVER trustpoint and to restore the keypair.

```
crypto ca import LOCAL-CA-SERVER pkcs12 <passphrase> (paste the pkcs12
base64 data here)
```



Note Be sure to use the exact name “LOCAL-CA-SERVER” for this step.

Step 3 If the LOCAL-CA-SERVER directory does not exist, you need to create it by entering **mkdir LOCAL-CA-SERVER**.

Step 4 Copy the local CA files into the LOCAL-CA-SERVER directory.

```
copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.ser
disk0:/LOCAL-CA-SERVER/
```

```
copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.cdb
disk0:/LOCAL-CA-SERVER/
```

```
copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.udb
disk0:/LOCAL-CA-SERVER/
```

```
copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.crl
disk0:/LOCAL-CA-SERVER/
```

```
copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.p12
disk0:/LOCAL-CA-SERVER/
```

Step 5 Enter the **crypto ca server** command to enable the local CA server

```
crypto ca server
  no shutdown
```

Step 6 Enter the **show crypto ca server** command to check that the local CA server is up and running.

Step 7 Save the configuration.

Restoring Configurations

You can specify configurations and images to restore from a zip file on your local computer.

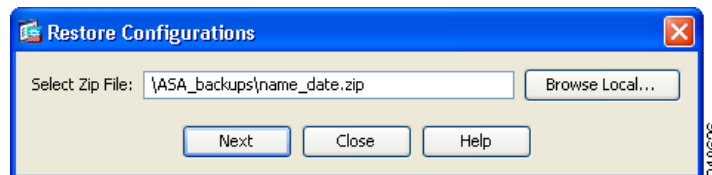
Before proceeding, note these other restrictions:

- The zip file that you restore must be created by choosing the Tools > Backup Configurations option.
- If you performed the backup with the master passphrase enabled, then you will need that master passphrase in order to restore the running configuration, start-up configuration, and VPN pre-shared keys from the backup you created. If you do not know the master passphrase for the ASA, those items will not be restored during the restore process. See the [“Configuring the Master Passphrase” section on page 14-5](#) for more information on master passphrases.
- If you specified a certificate passphrase during the backup, you will be asked to provide that passphrase in order to restore the certificates. The default passphrase is `cisco`.
- The DAP configuration may depend on a specific running configuration, URL list, and CSD configuration.
- The CSD configuration may depend on the version of the CSD image.
- You can restore components, images, and configurations using backups made from the same ASA type. You must start with a basic configuration that allows ASDM access.

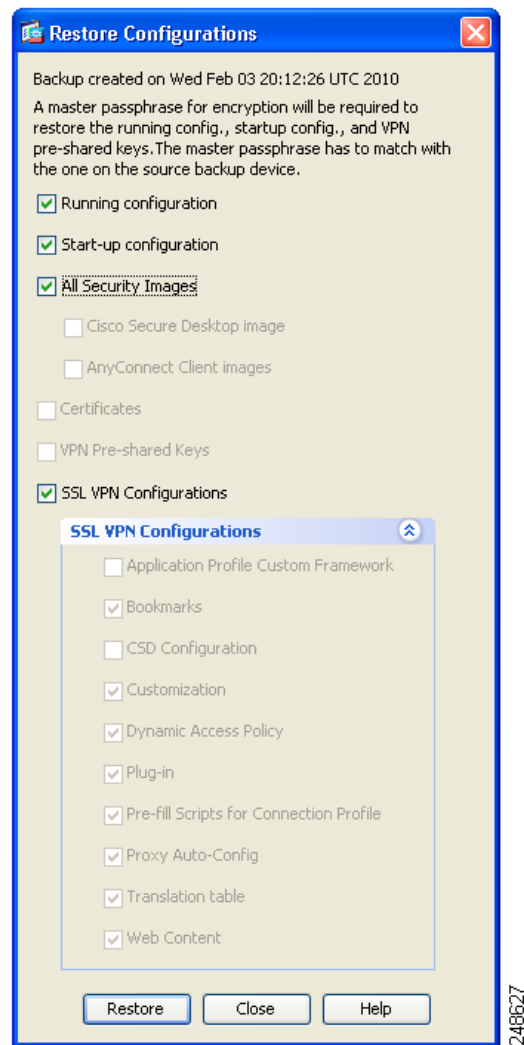
To restore selected elements of the ASA configuration, Cisco Secure Desktop image, or SSL VPN Client images and profiles, perform the following steps:

Step 1 Choose **Tools > Restore Configurations**.

Step 2 In the Restore Configurations dialog box, click **Browse Local Directory**, choose the zip file on your local computer that contains the configuration to restore, then click **Select**. The path and the zip filename appear in the Local File field.



Step 3 Click **Next**. The second Restore Configuration dialog box appears. Check the check boxes next to the configurations that you want to restore. All available SSL VPN configurations are selected by default.



Step 4 Click **Restore**.

Step 5 If you specified a certificate passphrase with which to encrypt the certificates when you created the backup file, ASDM prompts you to enter the passphrase.



Step 6 If you chose to restore the running configuration, you are asked if you want to merge the running configuration, replace the running configuration, or skip this part of the restoration process.

- Merging configurations combines the current running configuration and the backed-up running configuration.

- Replacing the running configuration uses the backed-up running configuration only.
- Skipping the step does not restore the backed-up running configuration.

ASDM displays a status dialog box until the restore operation is finished.

- Step 7** If you replaced or merged the running configuration, close ASDM and restart it. If you did not restore the running configuration or the running configuration, refresh the ASDM session for the changes to take effect.
-

Saving the Running Configuration to a TFTP Server

This feature stores a copy of the current running configuration file on a TFTP server.

To save the running configuration to a TFTP server, perform the following steps:

- Step 1** In the main ASDM application window, choose **File > Save Running Configuration to TFTP Server**. The Save Running Configuration to TFTP Server dialog box appears.
- Step 2** Enter the TFTP server IP address and file path on the TFTP server in which the configuration file will be saved, and then click **Save Configuration**.



Note To configure default TFTP settings, choose **Configuration > Device Management > Management Access > File Access > TFTP Client**. After you have configured this setting, the TFTP server IP address and file path on the TFTP server appear automatically in this dialog box.

Scheduling a System Restart

The System Reload tool lets you schedule a system restart or cancel a pending restart.

To schedule a system restart, perform the following steps:

- Step 1** In the main ASDM application window, choose **Tools > System Reload**.
- Step 2** In the Reload Scheduling area, define the following settings:
- a. For the Configuration State, choose either to save or discard the running configuration at restart time.
 - b. For the Reload Start Time, choose from the following options:
 - Click **Now** to perform an immediate restart.
 - Click **Delay by** to delay the restart by a specified amount of time. Enter the time before the restart begins in hours and minutes or only minutes.
 - Click **Schedule at** to schedule the restart to occur at a specific time and date. Enter the time of day the restart is to occur, and select the date of the scheduled restart.
 - c. In the Reload Message field, enter a message to send to open instances of ASDM at restart time.

- d. Check the **On reload failure force immediate reload after** check box to show the amount of time elapsed in hours and minutes or only minutes before a restart is attempted again.
- e. Click **Schedule Reload** to schedule the restart as configured.

The Reload Status area displays the status of the restart.

Step 3 Choose one of the following:

- Click **Cancel Reload** to stop a scheduled restart.
- Click **Refresh** to refresh the Reload Status display after a scheduled restart is finished.
- Click **Details** to display the results of a scheduled restart.

Downgrading Your Software

When you upgrade to Version 8.3, your configuration is migrated. The old configuration is automatically stored in flash memory. For example, when you upgrade from Version 8.2(1) to 8.3(1), the old 8.2(1) configuration is stored in flash memory in a file called 8_2_1_0_startup_cfg.sav.



Note

You must manually restore the old configuration before downgrading.

This section describes how to downgrade and includes the following topics:

- [Information About Activation Key Compatibility, page 84-28](#)
- [Performing the Downgrade, page 84-29](#)

Information About Activation Key Compatibility

Your activation key remains compatible if you upgrade to the latest version from any previous version. However, you might have issues if you want to maintain downgrade capability:

- Downgrading to Version 8.1 or earlier versions—After you upgrade, if you activate additional feature licenses that were introduced *before* 8.2, the activation key continues to be compatible with earlier versions if you downgrade. However if you activate feature licenses that were introduced in Version 8.2 or later versions, the activation key is not backwards compatible. If you have an incompatible license key, see the following guidelines:
 - If you previously entered an activation key in an earlier version, the ASA uses that key (without any of the new licenses you activated in Version 8.2 or later versions).
 - If you have a new system and do not have an earlier activation key, you need to request a new activation key compatible with the earlier version.
- Downgrading to Version 8.2 or earlier versions—Version 8.3 introduced more robust time-based key usage as well as failover license changes:
 - If you have more than one time-based activation key active, when you downgrade, only the most recently activated time-based key can be active. Any other keys are made inactive.
 - If you have mismatched licenses on a failover pair, downgrading will disable failover. Even if the keys are matching, the license used will no longer be a combined license.

Performing the Downgrade

See the [“The Backup and Restore features options on the Tools menu let you back up and restore the ASA running configuration, startup configuration, installed add-on images, and SSL VPN Client images and profiles.” section on page 84-20](#) for more information about configuration migration.

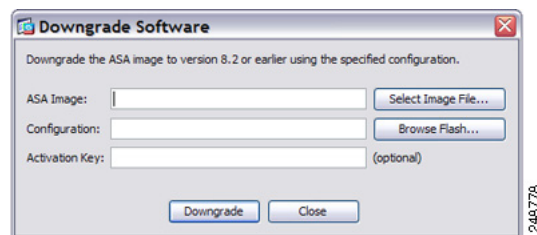
To downgrade from Version 8.3, perform the following steps:

Detailed Steps

Step 1 Choose **Tools > Downgrade Software**.

The Downgrade Software dialog box appears.

Figure 84-1 Downgrade Software



Step 2 For the ASA Image, click **Select Image File**.

The Browse File Locations dialog box appears.

Step 3 Click one of the following radio buttons:

- **Remote Server**—Choose **ftp**, **smb**, or **http** from the drop-down list, and type the path to the old image file.
- **Flash File System**—Click **Browse Flash** to choose the old image file on the local flash file system.

Step 4 For the Configuration, click **Browse Flash** to choose the pre-migration configuration file. (By default this was saved on disk0).

Step 5 (Optional) In the Activation Key field, enter the old activation key if you need to revert to a pre-8.3 activation key.

See the [“Information About Activation Key Compatibility” section on page 84-28](#) for more information.

Step 6 Click **Downgrade**.

This tool is a shortcut for completing the following functions:

1. Clearing the boot image configuration (**clear configure boot**).
2. Setting the boot image to be the old image (**boot system**).
3. (Optional) Entering a new activation key (**activation-key**).
4. Saving the running configuration to startup (**write memory**). This sets the BOOT environment variable to the old image, so when you reload, the old image is loaded.
5. Copying the old configuration to the startup configuration (**copy old_config_url startup-config**).
6. Reloading (**reload**).

Configuring Auto Update

This section includes the following topics:

- [Information About Auto Update, page 84-30](#)
- [Configuring Communication with an Auto Update Server, page 84-31](#)

Information About Auto Update

Auto Update is a protocol specification that allows an Auto Update Server to download configurations and software images to many ASAs and can provide basic monitoring of the ASAs from a central location.

The ASA can be configured as either a client or a server. As an Auto Update client, it periodically polls the Auto Update Server for updates to software images and configuration files. As an Auto Update Server, it issues updates for ASAs configured as Auto Update clients.

Auto Update is useful in solving many issues facing administrators for ASA management, such as:

- Overcoming dynamic addressing and NAT challenges.
- Committing configuration changes in one action.
- Providing a reliable method for updating software.
- Leveraging well-understood methods for high availability (failover).
- Providing flexibility with an open interface.
- Simplifying security solutions for Service Provider environments.

The Auto Update specification provides the infrastructure necessary for remote management applications to download ASA configurations, software images, and to perform basic monitoring from a centralized location or multiple locations.

The Auto Update specification allows the Auto Update server to either push configuration information and send requests for information to the ASA, or to pull configuration information by having the ASA periodically poll the Auto Update server. The Auto Update server can also send a command to the ASA to send an immediate polling request at any time. Communication between the Auto Update server and the ASA requires a communications path and local CLI configuration on each ASA.

Guidelines and Limitations

- If the ASA configuration is updated from an Auto Update server, ASDM is not notified. You must choose **Refresh** or **File > Refresh ASDM with the Running Configuration on the Device** to obtain the latest configuration, and any changes to the configuration made in ASDM will be lost.
- If HTTPS is chosen as the protocol to communicate with the Auto Update server, the ASA uses SSL, which requires the ASA to have a DES or 3DES license.
- Auto Update is supported in single context mode only.

Configuring Communication with an Auto Update Server

Detailed Steps

To configure the Auto Update feature, choose **Configuration > Device Management > System Image/Configuration > Auto Update**. The Auto Update pane consists of an Auto Update Servers table and two areas: the Timeout area and the Polling area.

The Auto Update Servers table lets you view the parameters of previously configured Auto Update servers. The ASA polls the server listed at the top of the table first. To change the order of the servers in the table, click **Move Up** or **Move Down**. The Auto Update Servers table includes the following columns:

- **Server**—The name or IP address of the Auto Update server.
- **User Name**—The user name used to access the Auto Update server.
- **Interface**—The interface used when sending requests to the Auto Update server.
- **Verify Certificate**—Indicates whether the ASA checks the certificate returned by the Auto Update server with the CA root certificates. The Auto Update server and the ASA must use the same CA.

Double-clicking any of the rows in the Auto Update Server table opens the Edit Auto Update Server dialog box, in which you can modify the Auto Update server parameters. These changes are immediately reflected in the table, but you must click **Apply** to save them to the configuration.

The Timeout area lets you set the amount of time the ASA waits for the Auto Update server to time out. The Timeout area includes the following fields:

- **Enable Timeout Period**—Check to enable the ASA to time out if no response is received from the Auto Update server.
- **Timeout Period (Minutes)**—Enter the number of minutes the ASA will wait to time out if no response is received from the Auto Update server.

The Polling area lets you configure how often the ASA will poll for information from the Auto Update server. The Polling area includes the following fields:

- **Polling Period (minutes)**—The number of minutes the ASA will wait to poll the Auto Update server for new information.
- **Poll on Specified Days**—Allows you to specify a polling schedule.
- **Set Polling Schedule**—Displays the Set Polling Schedule dialog box where you can configure the days and time-of-day to poll the Auto Update server.
- **Retry Period (minutes)**—The number of minutes the ASA will wait to poll the Auto Update server for new information if the attempt to poll the server fails.
- **Retry Count**—The number of times the ASA will attempt to retry to poll the Auto Update server for new information.

Adding or Editing an Auto Update Server

The Add/Edit Auto Update Server dialog box includes the following fields:

- **URL**—The protocol that the Auto Update server uses to communicate with the ASA, either HTTP or HTTPS, and the path to the Auto Update server.
- **Interface**—The interface to use when sending requests to the Auto Update server.
- **Verify Certificate**—Click to enable the ASA to verify the certificate returned by the Auto Update server with the CA root certificates. The Auto Update server and the ASA must use the same CA.

The User area includes the following fields:

- User Name (Optional)—Enter the user name needed to access the Auto Update server.
- Password—Enter the user password for the Auto Update server.
- Confirm Password—Reenter the user password for the Auto Update server.
- Use Device ID to uniquely identify the ASA—Enables authentication using a device ID. The device ID is used to uniquely identify the ASA to the Auto Update server.
- Device ID—Type of device ID to use.
 - Hostname—The name of the host.
 - Serial Number—The device serial number.
 - IP Address on interface—The IP address of the selected interface, used to uniquely identify the ASA to the Auto Update server.
 - MAC Address on interface—The MAC address of the selected interface, used to uniquely identify the ASA to the Auto Update server.
 - User-defined value—A unique user ID.

Setting the Polling Schedule

The Set Polling Schedule dialog box lets you configure specific days and the time-of-day for the ASA to poll the Auto Update server.

The Set Polling Schedule dialog box includes the following fields:

Days of the Week—Check the days of the week that you want the ASA to poll the Auto Update server.

The Daily Update pane group lets you configure the time of day when you want the ASA to poll the Auto Update server, and includes the following fields:

- Start Time—Enter the hour and minute to begin the Auto Update poll.
- Enable randomization—Check to enable the ASA to randomly choose a time to poll the Auto Update server.