



## Software and Configurations

---

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

- [Upgrading the Software, page 43-1](#)
- [Managing Files, page 43-8](#)
- [Configuring the Images and Startup Configuration to Use, page 43-18](#)
- [Backing Up and Restoring Configurations or Other Files, page 43-19](#)
- [Saving the Running Configuration to a TFTP Server, page 43-26](#)
- [Scheduling a System Restart, page 43-26](#)
- [Downgrading Your Software, page 43-27](#)
- [Configuring Auto Update, page 43-29](#)
- [Feature History for Software and Configurations, page 43-35](#)

### Upgrading the Software

- [Upgrade Path, page 43-1](#)
- [View Your Current Version, page 43-2](#)
- [Download the Software from Cisco.com, page 43-2](#)
- [Upgrade a Standalone Unit, page 43-2](#)
- [Upgrade a Failover Pair or ASA Cluster, page 43-5](#)

### Upgrade Path

See the following table for the upgrade path for your version. Some versions require an interim upgrade before you can upgrade to the latest version.



**Note**

There are no special requirements for Zero Downtime Upgrades for failover and ASA clustering with the following exception. Upgrading ASA clustering from 9.0(1) or 9.1(1): due to CSCue72961, hitless upgrading is not supported.

Current ASA Version	First Upgrade to:	Then Upgrade to:
8.2(x) and earlier	8.4(6)	9.2(1) or later
8.3(x)	8.4(6)	9.2(1) or later
8.4(1) through 8.4(4)	8.4(6), 9.0(4), or 9.1(2)	9.2(1) or later
8.4(5) and later	—	9.2(1) or later
8.5(1)	9.0(4) or 9.1(2)	9.2(1) or later
8.6(1)	9.0(4) or 9.1(2)	9.2(1) or later
9.0(1)	9.0(4) or 9.1(2)	9.2(1) or later
9.0(2) or later	—	9.2(1) or later
9.1(1)	9.1(2)	9.2(1) or later
9.1(2) or later	—	9.2(1) or later

### Configuration Migration

Depending on your current version, you might experience one or more configuration migrations when you upgrade. For example, when upgrading from 8.0 to 9.2, you will experience all of these migrations:

- 8.2—See the [8.2 release notes](#).
- 8.3—See the [Cisco ASA 5500 Migration Guide to Version 8.3](#).
- 8.4—See the [8.4 upgrade guide](#).
- 9.0—See the [9.0 upgrade guide](#).

## View Your Current Version

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

## Download 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/go/asa-software>

## Upgrade a Standalone Unit

This section describes how to install the ASDM and operating system (OS) images.

- [Upgrade from Your Local Computer, page 43-3](#)
- [Upgrade Using the Cisco.com Wizard, page 43-3](#)

## Upgrade from Your Local Computer

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.

### Procedure

- 
- 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** You are prompted to set this image as the ASDM image. Click **Yes**.
  - Step 8** You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the **Upgrade** tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.
  - Step 9** Repeat [Step 2](#) through [Step 8](#), choosing **ASA** from the **Image to Upload** drop-down list. You can also use this procedure to upload other file types.
  - Step 10** Choose **Tools > System Reload** to reload the ASA.

A new window appears that asks you to verify the details of the reload.

    - a. Click the **Save the running configuration at the time of reload** radio button (the default).
    - b. Choose a time to reload (for example, **Now**, the default).
    - c. 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.
- 

## Upgrade Using the Cisco.com Wizard

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 9.2(1), the download might be 9.2(1.2). 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.

### Procedure

---

**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 Cisco.com username and password, and then click **Login**.

The **Cisco.com Upgrade Wizard** appears.




---

**Note** If there is 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).

**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.

## Upgrade a Failover Pair or ASA Cluster

To perform a zero downtime upgrade, you need to upgrade each unit in a particular order.

- [Upgrade an Active/Standby Failover Pair, page 43-5](#)
- [Upgrade an Active/Active Failover Pair, page 43-6](#)
- [Upgrade an ASA Cluster, page 43-7](#)

### Upgrade an Active/Standby Failover Pair

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

#### Procedure

- 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** You are prompted to set this image as the ASDM image. Click **Yes**.
- Step 8** You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the **Upgrade** tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.
- Step 9** Repeat [Step 2](#) through [Step 8](#), choosing **ASA** from the **Image to Upload** drop-down list.
- Step 10** Click the **Save** icon on the toolbar to save your configuration changes.
- Step 11** Connect ASDM to the *standby* unit, and upload the ASA and ASDM software according to [Step 2](#) through [Step 9](#), using the same file locations you used on the active unit.
- Step 12** Choose **Tools > System Reload** to reload the standby ASA.  
A new window appears that asks you to verify the details of the reload.
  - a. Click the **Save the running configuration at the time of reload** radio button (the default).
  - b. Choose a time to reload (for example, **Now**, the default).
  - c. 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** After the standby ASA reloads, restart ASDM and connect to the standby unit to make sure it is running.
- Step 14** Connect ASDM to the *active* unit again.
- Step 15** Force the active unit to fail over to the standby unit by choosing **Monitoring > Properties > Failover > Status**, and clicking **Make Standby**.
- Step 16** Choose **Tools > System Reload** to reload the (formerly) active ASA.  
A new window appears that asks you to verify the details of the reload.
  - a. Click the **Save the running configuration at the time of reload** radio button (the default).
  - b. Choose a time to reload (for example, **Now**, the default).
  - c. 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.

---

## Upgrade an Active/Active Failover Pair

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

### Before You Begin

Perform these steps in the system execution space. .

### Procedure

---

- 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** You are prompted to set this image as the ASDM image. Click **Yes**.
- Step 8** You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the **Upgrade** tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.
- Step 9** Repeat [Step 2](#) through [Step 8](#), choosing **ASA** from the **Image to Upload** drop-down list.
- Step 10** Click the **Save** icon on the toolbar to save your configuration changes.

- Step 11** 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 12** Connect ASDM to the *secondary* unit, and upload the ASA and ASDM software according to [Step 2](#) through [Step 9](#), using the same file locations you used on the active unit.
- Step 13** 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 (the default).
  - Choose a time to reload (for example, **Now**, the default).
  - 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 14** Connect ASDM to the *primary* unit, and check when the secondary unit reloads by choosing **Monitoring > Failover > System**.
- Step 15** 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 16** 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 (the default).
  - Choose a time to reload (for example, **Now**, the default).
  - 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.
- 

## Upgrade 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.

### Procedure

- 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.

The **Upgrade Software** dialog box appears.

- Step 5** From the **Image to Upload** drop-down list, choose **ASDM**.
- 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.
- Step 9** You are prompted to set this image as the ASDM image. Click **Yes**.
- Step 10** You are reminded to exit ASDM and save the configuration. Click **OK**. You exit the Upgrade tool. **Note:** You will save the configuration and reload ASDM *after* you upgrade the ASA software.
- Step 11** Repeat [Step 3](#) through [Step 10](#), choosing **ASA** from the **Image to Upload** drop-down list.
- Step 12** Click the **Save** icon on the toolbar to save your configuration changes.
- Step 13** Choose **Tools > System Reload**.
- The System Reload dialog box appears.
- Step 14** Reload each slave unit one at a time by choosing a slave unit name from the Device drop-down list, and then clicking **Schedule Reload** to reload the unit now.
- To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up (approximately 5 minutes) before reloading the next unit. To view when a unit rejoins the cluster, see the **Monitoring > ASA Cluster > Cluster Summary** pane.
- Step 15** After all slave units have reloaded, disable clustering on the master unit by choosing **Configuration > Device Management > High Availability and Scalability > ASA Cluster**, uncheck the **Participate in ASA cluster** check box, and click **Apply**.
- Wait for 5 minutes for a new master to be selected and traffic to stabilize. When the former master unit rejoins the cluster, it will be a slave.
- Do not save the configuration; when the master unit reloads, you want clustering to be enabled on it.
- Step 16** Choose **Tools > System Reload** and reload the master unit from the System Reload dialog box by choosing **--This Device--** from the Device drop-down list.
- Step 17** 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.

- [Configuring File Access, page 43-9](#)
- [Accessing the File Management Tool, page 43-13](#)
- [Transferring Files, page 43-16](#)



## Configuring File Access

- [Configuring the FTP Client Mode, page 43-9](#)
- [Configuring the ASA as a Secure Copy Server, page 43-9](#)
- [Customizing the ASA Secure Copy Client, page 43-10](#)
- [Configuring the ASA TFTP Client Path, page 43-11](#)
- [Adding Mount Points, page 43-11](#)

### Configuring the FTP Client Mode

The ASA can use FTP to upload or download image files or configuration files to or from an FTP server. In passive FTP, the client initiates both the control connection and the data connection. The server, which is the recipient of the data connection in passive mode, responds with the port number to which it is listening for the specific connection.

#### Detailed Steps

---

**Step 1** From the Configuration > Device Management > Management Access > File Access > FTP Client pane, check the **Specify FTP mode as passive** check box.

**Step 2** Click **Apply**.

The FTP client configuration is changed and the change is saved to the running configuration.

---

### Configuring the ASA as a Secure Copy Server

You can enable the secure copy (SCP) server on the ASA. Only clients that are allowed to access the ASA using SSH can establish a secure copy connection.

#### Restrictions

- The server does not have directory support. The lack of directory support limits remote client access to the ASA internal files.
- The server does not support banners.
- The server does not support wildcards.

#### Prerequisites

- Enable SSH on the ASA according to the [Configuring Management Access, page 42-3](#).
- The ASA license must have the strong encryption (3DES/AES) license to support SSH Version 2 connections.

#### Detailed Steps

---

**Step 1** Choose **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server**, and check the **Enable secure copy server** check box.

**Step 2** Click **Apply**.**Example**

From a client on the external host, perform an SCP file transfer. For example, in Linux enter the following command:

```
scp -v -pw password source_filename username@asa_address:{disk0|disk1}:/dest_filename
```

The **-v** is for verbose, and if **-pw** is not specified, you will be prompted for a password.

**Customizing the ASA Secure Copy Client**

You can copy files to and from the ASA using the on-board SCP client (see [Accessing the File Management Tool, page 43-13](#)). This section lets you customize the SCP client operation.

**Prerequisites**

For multiple context mode, complete this procedure in the system execution space. If you are not already in the System configuration mode, in the Configuration > Device List pane, double-click **System** under the active device IP address.

**Detailed Steps**

**Step 1** Depending on your context mode:

- For single mode, choose **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP)**.
- For multiple mode in the System, choose **Configuration > Device Management > Device Administration > Secure Copy**

**Step 2** The ASA stores the SSH host key for each SCP server to which it connects. You can manually add or delete servers and their keys from the ASA database if desired.

To add a key:

- a. Click **Add** for a new server, or select the server from the Trusted SSH Hosts table, and click **Edit**.
- b. For a new server, in the Host field, enter the server IP address.
- c. Check the **Add public key for the trusted SSH host** check box.
- d. Specify one of the following keys:
  - Fingerprint—Enter the already hashed key; for example, a key that you copied from **show** command output.
  - Key—Enter the public key or hashed value of the SSH host. The key string is the Base64 encoded RSA public key of the remote peer. You can obtain the public key value from an open SSH client; that is, from the `.ssh/id_rsa.pub` file. After you submit the Base64 encoded public key, that key is then hashed via SHA-256.

To delete a key:

- a. Select the server from the Trusted SSH Hosts table, and click **Delete**.

**Step 3** To be informed when a new host key is detected, check the **Inform me when a new host key is detected** check box.

By default, this option is enabled. When this option is enabled, you are prompted to accept or reject the host key if it is not already stored on the ASA. When this option is disabled, the ASA accepts the host key automatically if it was not stored before.

**Step 4** Click **Apply**.

---

## Configuring the ASA TFTP Client Path

TFTP is a simple client/server file transfer protocol, which is described in RFC 783 and RFC 1350 Rev. 2. You can configure the ASA as a TFTP *client* so that it can copy files to or from a TFTP *server* (see [Transferring Files, page 43-16](#)). In this way, you can back up and propagate configuration files to multiple ASAs.

This section lets you pre-define the path to a TFTP server so you do not need to enter it in commands such as **copy** and **configure net**.

### Detailed Steps

- 
- Step 1** Choose **Configuration > Device Management > Management Access > File Access > TFTP Client**, and check the **Enable** check box.
- Step 2** From the Interface Name drop-down list, choose the interface to use as a TFTP client.
- Step 3** In the IP Address field, enter the IP address of the TFTP server on which configuration files will be saved.
- Step 4** In the Path field, enter the path to the TFTP server on which configuration files will be saved.  
For example: `/tftpboot/asa/config3`
- Step 5** Click **Apply**.
- 

## Adding Mount Points

This section includes the following topics:

- [Adding a CIFS Mount Point, page 43-11](#)
- [Adding an FTP Mount Point, page 43-12](#)

### Adding a CIFS Mount Point

To define a Common Internet File System (CIFS) mount point, perform the following steps:

- 
- Step 1** From the Configuration > Device Management > Management Access > File Access > Mount-Points pane, click **Add > CIFS Mount Point**.  
The Add CIFS Mount Point dialog box appears.
- Step 2** Check the **Enable mount point** check box.  
This option attaches the CIFS file system on the ASA to the UNIX file tree.
- Step 3** In the Mount Point Name field, enter the name of an existing CIFS location.

- Step 4** In the Server Name or IP Address field, enter the name or IP address of the server in which the mount point is located.
  - Step 5** In the Share Name field, enter the name of the folder on the CIFS server.
  - Step 6** In the NT Domain Name field, enter the name of the NT Domain in which the server resides.
  - Step 7** In the User Name field, enter the name of the user authorized for file system mounting on the server.
  - Step 8** In the Password field, enter the password for the user authorized for file system mounting on the server.
  - Step 9** In the Confirm Password field, reenter the password.
  - Step 10** Click **OK**.  
The Add CIFS Mount Point dialog box closes.
  - Step 11** Click **Apply**.  
The mount point is added to the ASA, and the change is saved to the running configuration.
- 

### Adding an FTP Mount Point



**Note** For an FTP mount point, the FTP server must have a UNIX directory listing style. Microsoft FTP servers have a default of the MS-DOS directory listing style.

---

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

- Step 1** From the Configuration > Device Management > Management Access > File Access > Mount-Points pane, click **Add > FTP Mount Point**.  
The Add FTP Mount Point dialog box appears.
- Step 2** Check the **Enable** check box.  
This option attaches the FTP file system on the ASA to the UNIX file tree.
- Step 3** In the Mount Point Name field, enter the name of an existing FTP location.
- Step 4** In the Server Name or IP Address field, enter the name or IP address of the server where the mount point is located.
- Step 5** In the Mode field, click the radio button for the FTP mode (**Active** or **Passive**). When you choose Passive mode, the client initiates both the FTP control connection and the data connection. The server responds with the number of its listening port for this connection.
- Step 6** In the Path to Mount field, enter the directory path name to the FTP file server.
- Step 7** In the User Name field, enter the name of the user authorized for file system mounting on the server.
- Step 8** In the Password field, enter the password for the user authorized for file system mounting on the server.
- Step 9** In the Confirm Password field, reenter the password.
- Step 10** Click **OK**.  
The Add FTP Mount Point dialog box closes.
- Step 11** Click **Apply**.

The mount point is added to the ASA, and the change is saved to the running configuration.

---

## 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 [Transferring Files, page 43-16](#) for more information.
- Step 10** Click **Mount Points** to open the Manage Mount Points dialog box. See [Managing Mount Points, page 43-13](#) 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 [Adding or Editing a CIFS/FTP Mount Point, page 43-14](#) 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 43-15](#).

This section includes the following topics:

- [Adding or Editing a CIFS/FTP Mount Point, page 43-14](#)

- [Accessing a CIFS Mount Point, page 43-15](#)

## 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-file systems 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 43-16](#)
- [Transferring Files Between Remote Server and Flash, page 43-16](#)

## 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

If you have more than one ASA or ASDM image, you should specify the image that you want to boot. If you do not set the image, the default boot image is used, and that image may not be the one intended. For the startup configuration, you can optionally specify a configuration file.

### Default Settings

#### ASA Image

- Physical ASA—Boots the first application image that it finds in internal flash memory.
- ASAv—Boots the image in the read-only boot:/ partition that was created when you first deployed. You can upgrade the image in flash memory and configure the ASAv to boot from that image. Note that if you later clear your configuration, then the ASAv will revert to loading the original deployment image.

#### ASDM Image

All ASAs—Boots the first ASDM image that it finds in internal flash memory, or if one does not exist in this location, then in external flash memory.

#### Startup Configuration

By default, the ASA boots from a startup configuration that is a hidden file.

### Detailed Steps

---

**Step 1** 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.

**Step 2** Click **Add** in the Boot Image/Configuration pane.

**Step 3** Browse to the image from which you want to boot. For a TFTP image, enter the TFTP URL in the File Name field. Click **OK**.

**Step 4** Arrange the images in order by using the Move Up and Move Down buttons.

**Step 5** (Optional) In the Boot Configuration File Path field, specify the startup configuration file by clicking **Browse Flash** and choosing the configuration. Click **OK**.

**Step 6** In the ASDM Image File Path field, specify the ASDM image by clicking **Browse Flash** and choosing the image. Click **OK**.

**Step 7** Click **Apply**.

---

# Backing Up and Restoring Configurations or Other Files

The Backup and Restore 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.

You can only restore a configuration to the same ASA version as when you performed the original backup. You cannot use the restore tool to migrate a configuration from one ASA version to another. If a configuration migration is required, the ASA automatically upgrades the resident startup configuration when it loads the new ASA OS.

- [Backing Up Configurations, page 43-19](#)
- [Backing Up the Local CA Server, page 43-22](#)
- [Restoring Configurations, page 43-23](#)
- [Saving the Running Configuration to a TFTP Server, page 43-26](#)

## Backing Up Configurations

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

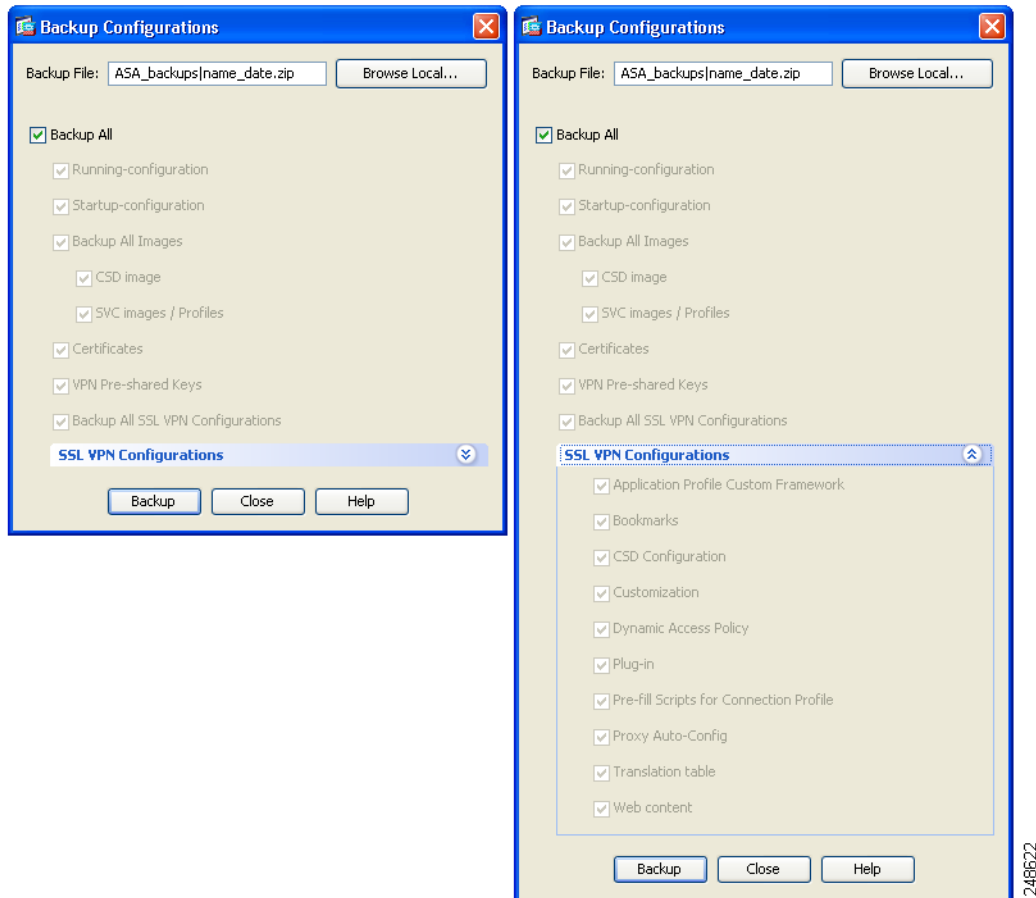
**Caution**

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 [Configuring the Master Passphrase, page 17-5](#) to learn how to reset it before continuing with the backup.

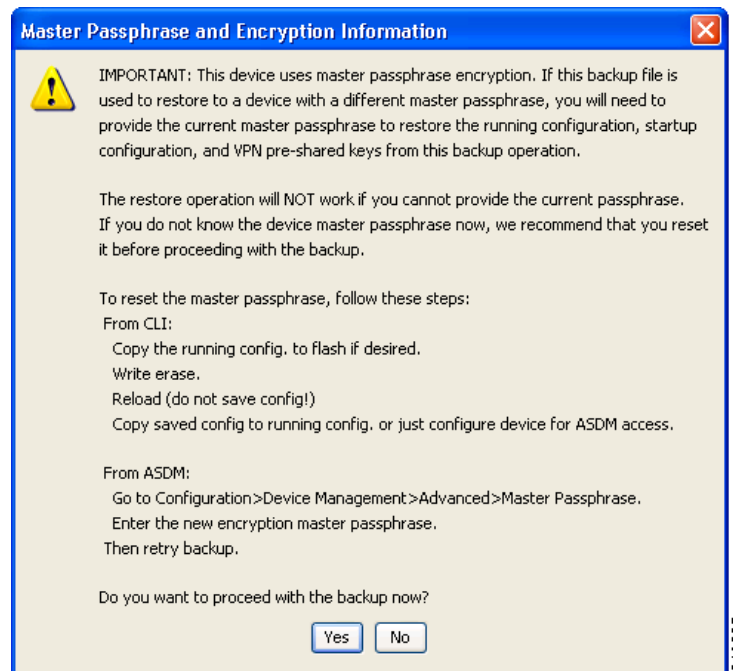
**Step 1** Create a folder on your computer to store backup files so they will be easy to find in case you need to restore them later.

**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](#), page 43-22.



- 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.ldb
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:

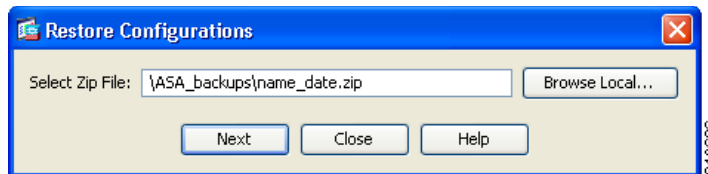
- The zip file that you restore must be created by choosing the Tools > Backup Configurations option.
- If you performed the backup with the master passphrase enabled, then you will need that master passphrase in order to restore the running configuration, start-up configuration, and VPN pre-shared keys 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 [Configuring the Master Passphrase, page 17-5](#) 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.
- If you import PKCS12 data (with the **crypto ca trustpoint** command) and the trustpoint uses RSA keys, the imported key pair is assigned the same name as the trustpoint. Because of this limitation, if you specify a different name for the trustpoint and its key pair after you have restored an ASDM configuration, the startup configuration will be the same as the original configuration, but the running configuration will include a different key pair name. This means that if you use different names for the key pair and trustpoint, you cannot restore the original configuration. To work around this issue, make sure that you use the same name for the trustpoint and its key pair.

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

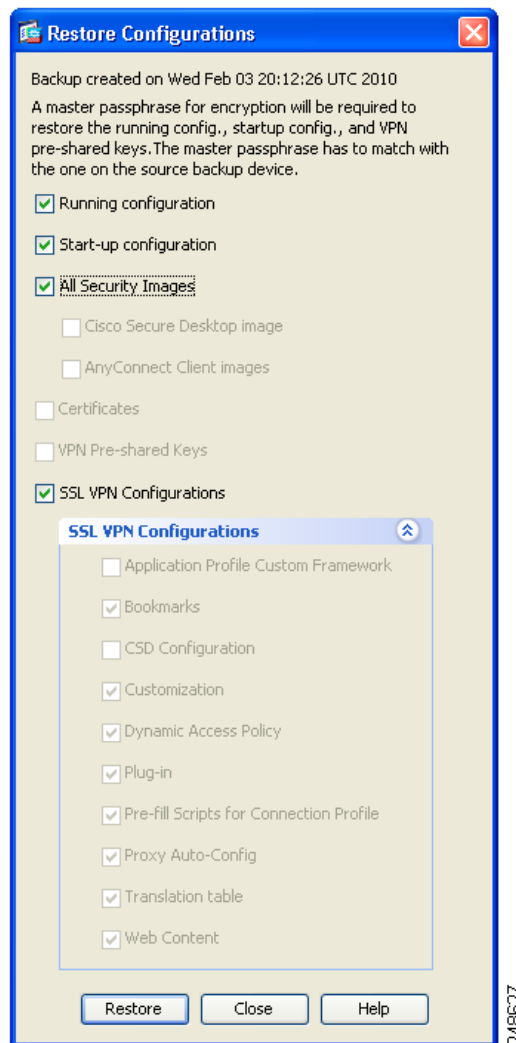
**Step 1** Choose **Tools > Restore Configurations**.

**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:
- For the Configuration State, choose either to save or discard the running configuration at restart time.
  - 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.
  - 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 43-27](#)
- [Performing the Downgrade, page 43-28](#)

## 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 Backup and Restore 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., [page 43-19](#) 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 43-1** 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 [Information About Activation Key Compatibility](#), [page 43-27](#) 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 43-29](#)
- [Guidelines and Limitations, page 43-32](#)
- [Configuring Communication with an Auto Update Server, page 43-32](#)

## 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.

- [Auto Update Client or Server, page 43-29](#)
- [Auto Update Benefits, page 43-29](#)
- [Auto Update Server Support in Failover Configurations, page 43-30](#)

## Auto Update Client or Server

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 Benefits

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.

## Auto Update Server Support in Failover Configurations

You can use the Auto Update Server to deploy software images and configuration files to ASAs in an Active/Standby failover configuration. To enable Auto Update on an Active/Standby failover configuration, enter the Auto Update Server configuration on the primary unit in the failover pair.

The following restrictions and behaviors apply to Auto Update Server support in failover configurations:

- Only single mode, Active/Standby configurations are supported.
- When loading a new platform software image, the failover pair stops passing traffic.
- When using LAN-based failover, new configurations must not change the failover link configuration. If they do, communication between the units will fail.
- Only the primary unit will perform the call home to the Auto Update Server. The primary unit must be in the active state to call home. If it is not, the ASA automatically fails over to the primary unit.
- Only the primary unit downloads the software image or configuration file. The software image or configuration is then copied to the secondary unit.
- The interface MAC address and hardware-serial ID is from the primary unit.
- The configuration file stored on the Auto Update Server or HTTP server is for the primary unit only.

### Auto Update Process Overview

The following is an overview of the Auto Update process in failover configurations. This process assumes that failover is enabled and operational. The Auto Update process cannot occur if the units are synchronizing configurations, if the standby unit is in the failed state for any reason other than SSM card failure, or if the failover link is down.

1. Both units exchange the platform and ASDM software checksum and version information.
2. The primary unit contacts the Auto Update Server. If the primary unit is not in the active state, the ASA first fails over to the primary unit and then contacts the Auto Update Server.
3. The Auto Update Server replies with software checksum and URL information.
4. If the primary unit determines that the platform image file needs to be updated for either the active or standby unit, the following occurs:
  - a. The primary unit retrieves the appropriate files from the HTTP server using the URL from the Auto Update Server.
  - b. The primary unit copies the image to the standby unit and then updates the image on itself.
  - c. If both units have new image, the secondary (standby) unit is reloaded first.
    - If hitless upgrade can be performed when secondary unit boots, then the secondary unit becomes the active unit and the primary unit reloads. The primary unit becomes the active unit when it has finished loading.
    - If hitless upgrade cannot be performed when the standby unit boots, then both units reload at the same time.
  - d. If only the secondary (standby) unit has new image, then only the secondary unit reloads. The primary unit waits until the secondary unit finishes reloading.
  - e. If only the primary (active) unit has new image, the secondary unit becomes the active unit, and the primary unit reloads.
  - f. The update process starts again at Step 1.

5. If the ASA determines that the ASDM file needs to be updated for either the primary or secondary unit, the following occurs:
  - a. The primary unit retrieves the ASDM image file from the HTTP server using the URL provided by the Auto Update Server.
  - b. The primary unit copies the ASDM image to the standby unit, if needed.
  - c. The primary unit updates the ASDM image on itself.
  - d. The update process starts again at Step 1.
6. If the primary unit determines that the configuration needs to be updated, the following occurs:
  - a. The primary unit retrieves the configuration file from the using the specified URL.
  - b. The new configuration replaces the old configuration on both units simultaneously.
  - c. The update process begins again at Step 1.
7. If the checksums match for all image and configuration files, no updates are required. The process ends until the next poll time.

### Monitoring the Auto Update Process

You can use the **debug auto-update client** or **debug fover cmd-exe** commands to display the actions performed during the Auto Update process. The following is sample output from the **debug auto-update client** command. Run **debug** commands from a terminal session.

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
  Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
  Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
  Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msecs
Auto-update client: update img on active unit...
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
```

```

auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
auto-update: HA safe reload: reload active waiting with mate state: 50

auto-update: HA safe reload: reload active waiting with mate state: 80
  Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419

```

The following syslog message is generated if the Auto Update process fails:

```
%ASA4-612002: Auto Update failed: file version: version reason: reason
```

The *file* is “image”, “asdm”, or “configuration”, depending on which update failed. The *version* is the version number of the update. And the *reason* is the reason that the update failed.

## 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.
- **Do not verify server's SSL certificate**—Check to disable the verification of 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.

# Feature History for Software and Configurations

Table 43-1 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

**Table 43-1** Feature History for Software and Configurations

Feature Name	Platform Releases	Feature Information
Secure Copy client	9.1(5)/9.2(1)	<p>The ASA now supports the Secure Copy (SCP) client to transfer files to and from a SCP server.</p> <p>We modified the following screens:</p> <p>Tools &gt; File Management &gt; File Transfer &gt; Between Remote Server and Flash</p> <p><b>Configuration &gt; Device Management &gt; Management Access &gt; File Access &gt; Secure Copy (SCP) Server</b></p>
Auto Update server certificate verification enabled by default	9.2(1)	<p>The Auto Update server certificate verification is now enabled by default; for new configurations, you must explicitly disable certificate verification. If you are upgrading from an earlier release, and you did not enable certificate verification, then certificate verification is not enabled, and you see the following warning:</p> <pre>WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.</pre> <p>The configuration will be migrated to explicitly configure no verification.</p> <p>We modified the following screen: Configuration &gt; Device Management &gt; System/Image Configuration &gt; Auto Update &gt; Add Auto Update Server.</p>

