



CHAPTER 55

Managing Software and Configurations

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

- [Saving the Running Configuration to a TFTP Server, page 55-1](#)
- [Managing Files, page 55-2](#)
- [Configuring Auto Update, page 55-7](#)
- [Configuring the Boot Image/Configuration Settings, page 55-9](#)
- [Upgrading Software from Your Local Computer, page 55-10](#)
- [Upgrading Software from the Cisco.com Wizard, page 55-11](#)
- [Scheduling a System Restart, page 55-12](#)
- [Backing Up and Restoring Configurations, Images, and Profiles \(Single Mode\), page 55-13](#)
- [Downgrading Your Software, page 55-20](#)

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.

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.

This section includes the following topics:

- [Accessing the File Management Tool, page 55-2](#)
- [Managing Mount Points, page 55-3](#)
- [Transferring Files, page 55-5](#)

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 55-5](#) for more information.
- Step 10** Click **Mount Points** to open the Manage Mount Points dialog box. See the [“Managing Mount Points” section on page 55-3](#) 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 55-3](#) 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 55-4](#).

**Note**

On a PIX 535 security appliance in single, routed mode, the Managing Mount Point feature is not available.

This section includes the following topics:

- [Adding or Editing a CIFS/FTP Mount Point, page 55-3](#)
- [Accessing a CIFS Mount Point, page 55-4](#)

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 ASASM 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 ASASM. You can transfer a remote file to and from the ASASM using HTTP, HTTPS, TFTP, FTP, or SMB.

- [Transferring Files Between Local PC and Flash, page 55-5](#)
- [Transferring Files Between Remote Server and Flash, page 55-6](#)

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 Auto Update

This section includes the following topics:

- [Setting the Polling Schedule, page 55-8](#)
- [Adding or Editing an Auto Update Server, page 55-9](#)

The Auto Update pane lets you configure the ASASM to be managed remotely from servers that support the Auto Update specification. Auto Update lets you apply configuration changes to the ASASM and receive software updates from remote locations.

Auto Update is useful in solving many issues facing administrators for ASASM 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 ASASM 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 ASASM, or to pull configuration information by having the ASASM periodically poll the Auto Update Server. The Auto Update Server can also send a command to the ASASM to send an immediate polling request at any time. Communication between the Auto Update Server and the ASASM requires a communications path and local CLI configuration on each ASASM.

Important Notes

- If the ASASM 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 ASASM uses SSL, which requires the ASASM to have a DES or 3DES license.

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 ASASM 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 ASASM checks the certificate returned by the Auto Update Server with the CA root certificates. The Auto Update Server and the ASASM 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 ASASM waits for the Auto Update Server to time out. The Timeout area includes the following fields:

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

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

- **Polling Period (minutes)**—The number of minutes the ASASM 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 ASASM 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 ASASM will attempt to retry to poll the Auto Update Server for new information.

Setting the Polling Schedule

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

The Daily Update pane group lets you configure the time of day when you want the ASASM 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 ASASM to randomly choose a time to poll the Auto Update Server.

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 ASASM, 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 ASASM to verify the certificate returned by the Auto Update Server with the CA root certificates. The Auto Update Server and the ASASM 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 ASASM 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 ASASM to the Auto Update Server.
 - MAC Address on interface—The MAC address of the selected interface, used to uniquely identify the ASASM to the Auto Update Server.
 - User-defined value—A unique user ID.

Configuring the Boot Image/Configuration Settings

The Boot Image/Configuration pane lets you choose which image file the ASASM will boot from, as well as the configuration file to use at startup. 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 55-10](#).
- **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.

Upgrading Software from Your Local Computer

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

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

-
- Step 1** In the main ASDM application window, choose **Tools > Upgrade Software from Local Computer**. The Upgrade Software from Local Computer dialog box appears.
 - Step 2** Choose the image file to upload from the drop-down list.
 - Step 3** Enter the local path to the file on your PC or click **Browse Local Files** to find the file on your PC.
 - Step 4** Enter the path to the flash file system or click **Browse Flash** to find the directory or file in the flash file system.
 - Step 5** Click **Image to Upload**. The uploading process might take a few minutes; make sure you wait until it is finished.
-

Upgrading Software from the Cisco.com Wizard

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

**Note**

This feature is only available in single mode and in the system space of multiple security mode. It is not available in a user or admin context.

In this wizard, you can do the following:

- Choose an ASA image file and/or ASDM image file to 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 ASASM to save the configuration and complete the upgrade.

To upgrade software from Cisco.com, perform the following steps:

Step 1 In the main ASDM application window, choose **Tools > Check for ASA/ASDM Updates**.

The Cisco.com Authentication dialog box appears.

Step 2 Enter your assigned Cisco.com username and the Cisco.com password, and then click **Login**.

A Status dialog box appears, indicating that ASDM is loading the Upgrade Wizard. The Cisco.com Upgrade Wizard appears. The Overview screen describes the steps in the image upgrade installation process.

Step 3 Click **Next** to display the Select Software screen.

The current ASA version and ASDM version appear.

Step 4 To upgrade the ASA version and ASDM version, perform the following steps:

- a. 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.
- b. 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.

**Note**

If the ASASM version list or the ASDM version list is empty, a statement appears informing you that no new ASASM or ASDM images are available and your device software is up-to-date. If you see this statement, you can exit the wizard.

Step 5 Click **Next** to display the Review Changes screen.

Step 6 Verify the following items:

- The ASASM image file and/or ASDM image file that you have downloaded are the correct ones.

**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.

- The ASASM image file and/or ASDM image file that you want to upload are the correct ones.
- The correct ASASM boot image has been selected.

Step 7 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 ASASM and is saved in the bootup error log file. All previously saved configuration files are also removed.

Step 8 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 ASASM, and restart ASDM.

Step 9 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.

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.
- 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.
- 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.
-

Backing Up and Restoring Configurations, Images, and Profiles (Single Mode)

The Backup and Restore features options on the Tools menu let you back up and restore the ASASM 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.

This section includes the following topics:

- [Backing Up Configurations, page 55-13](#)
- [Backing Up the Local CA Server, page 55-16](#)
- [Restoring Configurations, page 55-17](#)

Backing Up Configurations

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



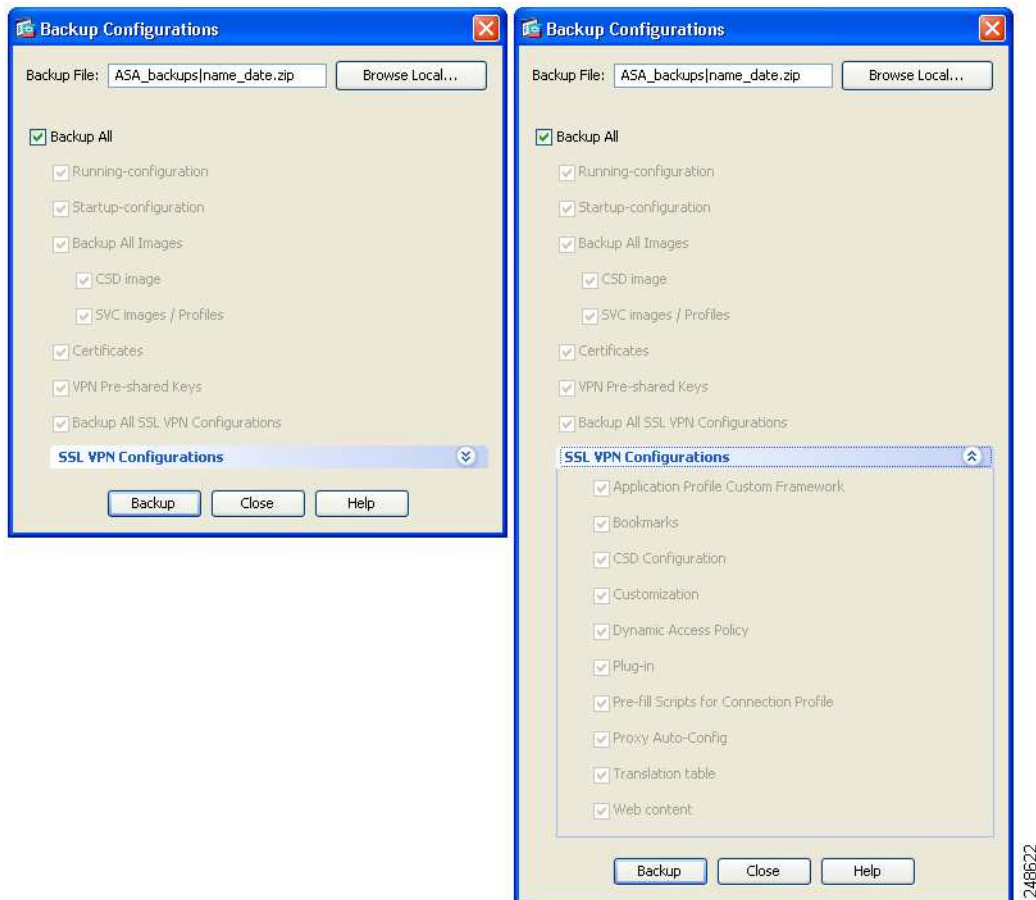
Caution

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 12-3](#) to learn how to reset it before continuing with the backup.

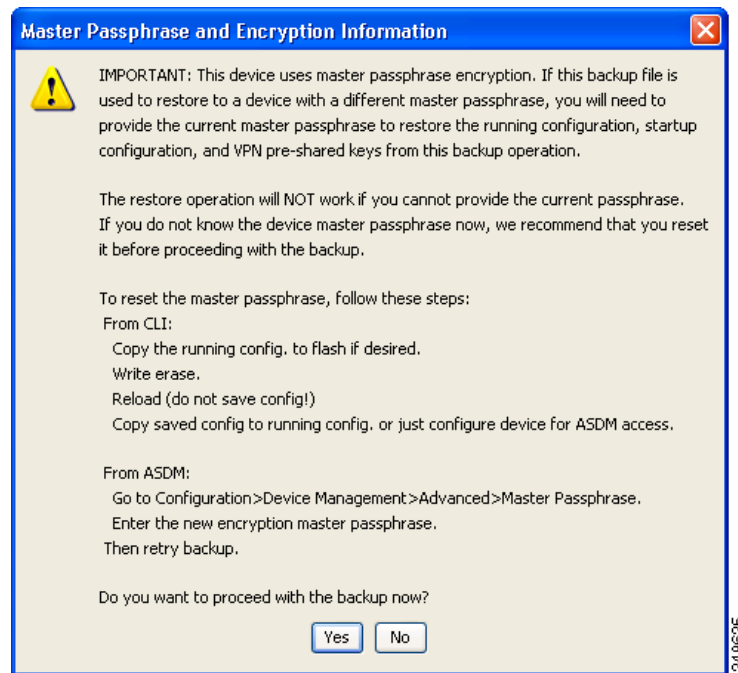
Step 1 Create a folder on your computer to store backup files so they will be easy to find in case you need to restore them later.

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 the [“Backing Up the Local CA Server”](#) section on page 55-16.



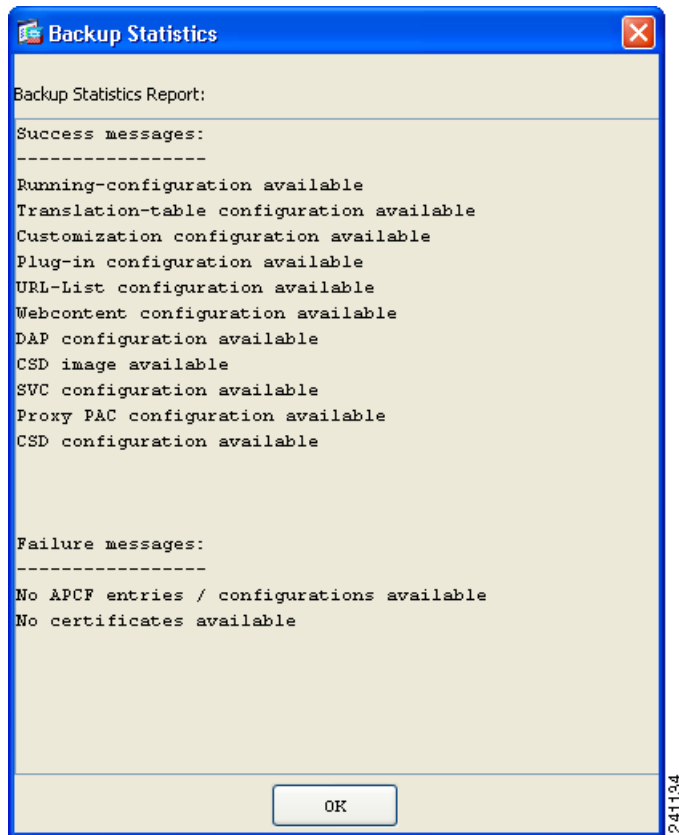
- To encrypt certificates, enter and confirm your certificate passphrase in the Certificate Passphrase dialog box and click **OK**. You will need to remember the password you enter in this dialog box when restoring the certificates.
- Clicking **Cancel** skips the step and does not back up certificates.

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 perform 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:

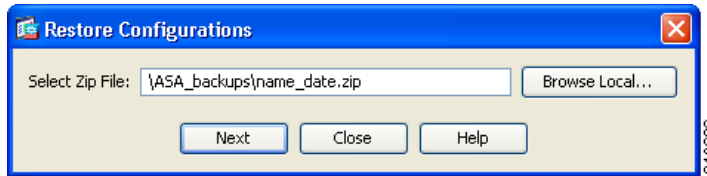
- The zip file that you restore must be created by choosing the Tools > Backup Configurations option.
- If you performed the backup with the master passphrase enabled, then you will need that master passphrase in order to restore the running configuration, start-up configuration, and VPN pre-shared keys 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 the [“Configuring the Master Passphrase” section on page 12-3](#) 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 ASASM type. You must start with a basic configuration that allows ASDM access.

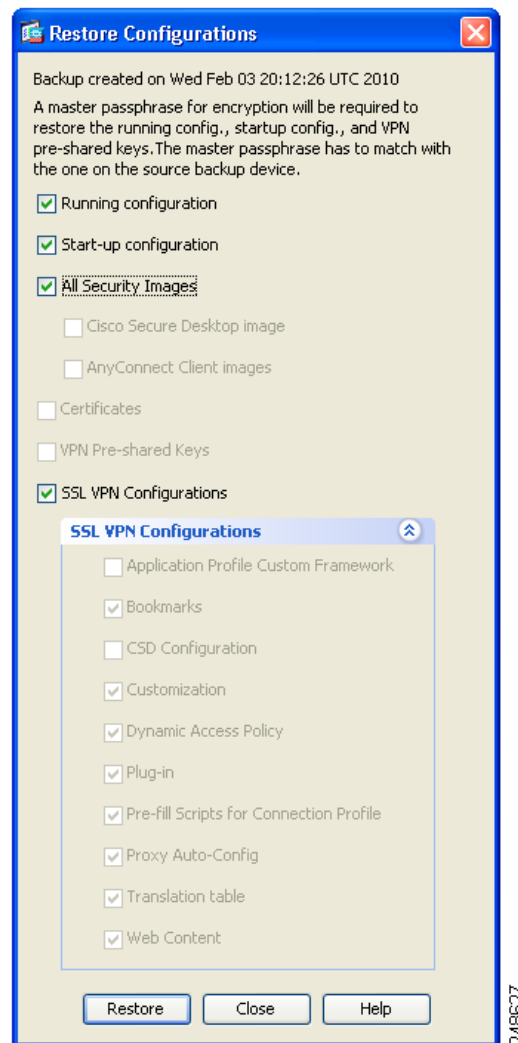
To restore selected elements of the ASASM configuration, Cisco Secure Desktop image, or SSL VPN Client images and profiles, perform the following steps:

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.

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 55-20](#)
- [Performing the Downgrade, page 55-21](#)

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 backward compatible. If you have an incompatible license key, see the following guidelines:
 - If you previously entered an activation key in an earlier version, the ASASM 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 [“Backing Up and Restoring Configurations, Images, and Profiles \(Single Mode\)”](#) section on page 55-13 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.



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 55-20 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**).

