# Software and Configurations

This chapter describes how to manage the Cisco ASA software and configurations.


- Upgrade the Software, on page 1
- Load an Image Using ROMMON, on page 1
- Load an Image for the ASASM Using ROMMON, on page 3
- Upgrade the ROMMON Image (ASA 5506-X, 5508-X, and 5516-X, ISA 3000), on page 4
- Recover and Load an Image for the ASA 5506W-X Wireless Access Point, on page 6
- Downgrade Your Software, on page 6
- Manage Files, on page 10
- Set the ASA Image, ASDM, and Startup Configuration, on page 17
- Back Up and Restore Configurations or Other Files, on page 19
- Schedule a System Restart, on page 25
- Configure Auto Update, on page 26
- History for Software and Configurations, on page 32


# Upgrade the Software

See the Cisco ASA Upgrade Guide for full upgrade procedures.

# Load an Image Using ROMMON

To load a software image onto an ASA from the ROMMON mode using TFTP, perform the following steps.

**Procedure**

**Step 1** Connect to the ASA console port according to the instructions in Access the Appliance Console.

**Step 2** Power off the ASA, then power it on.

**Step 3** During startup, press the **Escape** key when you are prompted to enter ROMMON mode.

**Step 4** In ROMMOM mode, define the interface settings to the ASA, including the IP address, TFTP server address, gateway address, software image file, and port, as follows:

```
rommon #1> interface gigabitethernet0/0
```

```
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

**Note** Be sure that the connection to the network already exists.

The **interface** command is ignored on the ASA 5506-X, ASA 5508-X, and ASA 5516-X platforms, and you must perform TFTP recovery on these platforms from the Management 1/1 interface.

**Step 5** Validate your settings:

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

**Step 6** Ping the TFTP server:

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

**Step 7** Save the network settings for future use:

```
rommon #8> sync
Updating NVRAM Parameters...
```

**Step 8** Load the software image:

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
```

```
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

After the software image is successfully loaded, the ASA automatically exits ROMMON mode.

**Step 9** Booting the ASA from ROMMON mode does not preserve the system image across reloads; you must still download the image to flash memory. See Upgrade the Software, on page 1.

# Load an Image for the ASASM Using ROMMON

To load a software image to an ASASM from the ROMMON mode using TFTP, perform the following steps.

**Procedure**

**Step 1** Connect to the ASA console port according to the instructions in Access the ASA Services Module Console.

**Step 2** Make sure that you reload the ASASM image.

**Step 3** During startup, press the **Escape** key when you are prompted to enter ROMMON mode.

**Step 4** In ROMMOM mode, define the interface settings to the ASASM, including the IP address, TFTP server address, gateway address, software image file, port, and VLAN, as follows:

```
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
rommon #5> interface Data0
rommon #6> vlan 1
Data0
Link is UP
MAC Address: 0012.d949.15b8
```

**Note** Be sure that the connection to the network already exists.

**Step 5** Validate your settings:

```
rommon #7> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.4
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=Data0
  VLAN=1
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
  RETRY=20
```

**Step 6** Ping the TFTP server:

```
rommon #8> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 2 seconds:

Success rate is 100 percent (20/20)
```

**Step 7** Load the software image:

```
rommon #9> tftpdnld
Clearing EOBC receive queue ...
cmostime_set = 1
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=Data0
  VLAN=1
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21
Starting download. Press ESC to abort.
```

After the software image is successfully loaded, the ASASM automatically exits ROMMON mode.

**Step 8** Booting the module from ROMMON mode does not preserve the system image across reloads; you must still download the image to flash memory. See Upgrade the Software, on page 1.

# Upgrade the ROMMON Image (ASA 5506-X, 5508-X, and 5516-X, ISA 3000)

Follow these steps to upgrade the ROMMON image for the ASA 5506-X series, ASA 5508-X, ASA 5516-X, and ISA 3000. For the ASA models, the ROMMON version on your system must be 1.1.8 or greater. We recommend that you upgrade to the latest version.

You can only upgrade to a new version; you cannot downgrade.

**Caution** The ASA 5506-X, 5508-X, and 5516-X ROMMON upgrade for 1.1.15 and the ISA 3000 ROMMON upgrade for 1.0.5 takes twice as long as previous ROMMON versions, approximately 15 minutes. **Do not** power cycle the device during the upgrade. If the upgrade is not complete within 30 minutes or it fails, contact Cisco technical support; **do not** power cycle or reset the device.

### Before you begin

Obtain the new ROMMON image from Cisco.com, and put it on a server to copy to the ASA. The ASA supports FTP, TFTP, SCP, HTTP(S), and SMB servers. Download the image from:

- ASA 5506-X, 5508-X, 5516-X: https://software.cisco.com/download/home/286283326/type
- ISA 3000: https://software.cisco.com/download/home/286288493/type

### Procedure

**Step 1** Copy the ROMMON image to the ASA flash memory. This procedure shows an FTP copy; enter **copy ?** for the syntax for other server types.

**copy ftp://**[*username***:***password***@**]*server_ip***/asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

**Step 2** To see your current version, enter the **show module** command and look at the Fw Version in the output for Mod 1 in the MAC Address Range table:

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

**Step 3** Upgrade the ROMMON image:

**upgrade rommon disk0:asa5500-firmware-***xxxx***.SPA**

**Example:**

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

**Step 4** Confirm to reload the ASA when you are prompted.

The ASA upgrades the ROMMON image, and then reloads the operating system.

# Recover and Load an Image for the ASA 5506W-X Wireless Access Point

To recover and load a software image onto an ASA 5506W-X using TFTP, perform the following steps.

**Procedure**

**Step 1** Session to the access point (AP) and enter the AP ROMMON (not the ASA ROMMON):

```
ciscoasa# hw-module module wlan recover image
```

**Step 2** Follow the procedure in the Cisco IOS Software Configuration Guide for Cisco Aironet Access Points.

# Downgrade Your Software

In many cases, you can downgrade your ASA software and restore a backup configuration from the previous software version. The method of downgrading depends on your ASA platform.

## Guidelines and Limitations for Downgrading

See the following guidelines before downgrading:

- There is no official Zero Downtime Downgrade support for clustering. However, in some cases, Zero Downtime Downgrading will work. See the following known issues for downgrading; note that there may be other issues that require you to reload your cluster units, thus causing downtime.
  - Downgrade to a pre-9.9(1) release with clustering—9.9(1) and later includes an improvement in the backup distribution. If you have 3 or more units in the cluster, you must perform the following steps:
    1. Remove all secondary units from the cluster (so the cluster consists only of the primary unit).
    2. Downgrade 1 secondary unit, and rejoin it to the cluster.
    3. Disable clustering on the primary unit; downgrade it, and rejoin the cluster.
    4. Downgrade the remaining secondary units, and join them back to the cluster, one at a time.
  - Downgrade to a pre-9.9(1) release when you enable cluster site redundancy—You should disable site redundancy if you want to downgrade (or if you want to add a pre-9.9(1) unit to a cluster). Otherwise, you will see side effects, for example, dummy forwarding flows on the unit running the old version.

  - Downgrade from 9.8(1) with clustering and crypto-map—There is no Zero Downtime Downgrade support when downgrading from 9.8(1) when you have a crypto-map configured. You should clear the crypto-map configuration before downgrading, and then re-apply the configuration after the downgrade.
  - Downgrade from 9.8(1) with clustering unit health check set to .3 to .7 seconds—If you downgrade your ASA software after setting the hold time to .3 - .7 (**health-check holdtime**), this setting will revert to the default of 3 seconds because the new setting is unsupported.
  - Downgrade from 9.5(2) or later to 9.5(1) or earlier with clustering (CSCuv82933)—There is no Zero Downtime Downgrade support when downgrading from 9.5(2). You must reload all units at roughly the same time so that a new cluster is formed when the units come back online. If you wait to reload the units sequentially, then they will be unable to form a cluster.
  - Downgrade from 9.2(1) or later to 9.1 or earlier with clustering—Zero Downtime Downgrade is not supported.

- Downgrade from 9.10(1) for smart licensing—Due to changes in the smart agent, if you downgrade, you must re-register your device to the Cisco Smart Software Manager. The new smart agent uses an encrypted file, so you need to re-register to use an unencrypted file required by the old smart agent.
- Downgrade to 9.5 and earlier with passwords using PBKDF2 (Password-Based Key Derivation Function 2) hash—Versions before 9.6 do not support PBKDF2 hashing. In 9.6(1), **enable** and **username** passwords longer than 32 characters use PBKDF2 hashing. In 9.7(1), new passwords of all lengths use PBKDF2 hashing (existing passwords continue to use MD5 hashing). If you downgrade, the **enable** password reverts to the default (which is blank). Usernames will not parse correctly, and the **username** commands will be removed. You must re-create your local users.
- Downgrade from Version 9.5(2.200) for the ASAv—The ASAv does not retain the licensing registration state. You need to re-register with the **license smart register idtoken id_token force** command (for ASDM: see the **Configuration > Device Management > Licensing > Smart Licensing** page, and use the **Force registration** option); obtain the ID token from the Smart Software Manager.
- VPN tunnels are replicated to the standby unit even if the standby unit is running a version of software that does not support the Ciphersuite that the original tunnel negotiated. This scenario occurs when downgrading. In this case, disconnect your VPN connection and reconnect.

# Incompatible Configuration Removed After Downgrading

When you downgrade to an old version, commands that were introduced in later versions will be removed from the configuration. There is no automated way to check the configuration against the target version before you downgrade. You can view when new commands were added in ASA new features by release.

You can view rejected commands *after* you downgrade using the **show startup-config errors** command. If you can perform a downgrade on a lab device, you can preview the effects using this command before you perform the downgrade on a production device.

In some cases, the ASA migrates commands to new forms automatically when you upgrade, so depending on your version, even if you did not manually configure new commands, the downgrade could be affected by configuration migrations. We recommend that you have a backup of your old configuration that you can use when you downgrade. In the case of upgrading to 8.3, a backup is automatically created (<old_version>_startup_cfg.sav). Other migrations do not create back-ups. See the "Version-Specific Guidelines

and Migrations" in the ASA Upgrade guide for more information about automatic command migrations that could affect downgrading.

See also known downgrade issues in Guidelines and Limitations for Downgrading, on page 6.

For example, an ASA running version 9.8(2) includes the following commands:

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
```

When you downgrade to 9.0(4), you will see the following errors on startup:

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
                                  ^
ERROR: % Invalid input detected at '^' marker.

username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                                ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted auth
 md5 12:ab:34 priv aes 128 12:ab:34
                                       ^
ERROR: % Invalid input detected at '^' marker.
```

In this example, support for **sctp** in the **access-list extended** command was added in version 9.5(2), support for **pbkdf2** in the **username** command was added in version 9.6(1), and support for **engineID** in the **snmp-server user** command was added in version 9.5(3).

# Downgrade the Firepower 2100

You can downgrade the ASA software version by restoring the backup configuration to the startup configuration, setting the ASA version to the old version, and then reloading.

### Before you begin

This procedure requires a backup configuration of the ASA before you upgraded, so you can restore the old configuration. If you do not restore the old configuration, you may have incompatible commands representing new or changed features. Any new commands will be rejected when you load the old software version.

### Procedure

**Step 1** At the ASA CLI, copy the backup ASA configuration to the startup configuration. For failover, perform this step on the active unit. This step replicates the command to the standby unit.

**copy** *old_config_url* **startup-config**

It's important that you do not save the running configuration to the startup configuration using **write memory**; this command will overwrite your backup configuration.

**Example:**

```
ciscoasa# copy disk0:/9.12.4_cfg.sav startup-config
```

**Step 2** In FXOS, use the Firepower Chassis Manager or FXOS CLI to use the old ASA software version using the upgrade procedure in the ASA upgrade guide for standalone, failover, or clustering deployments. In this case, specify the old ASA version instead of a new version.

# Downgrade the Firepower 4100/9300

You can downgrade the ASA software version by restoring the backup configuration to the startup configuration, setting the ASA version to the old version, and then reloading.

### Before you begin

- This procedure requires a backup configuration of the ASA before you upgraded, so you can restore the old configuration. If you do not restore the old configuration, you may have incompatible commands representing new or changed features. Any new commands will be rejected when you load the old software version.
- Make sure the old ASA version is compatibile with the current FXOS version. If not, downgrade FXOS as the first step before you restore the old ASA configuration. Just make sure the downgraded FXOS is also compatible with the current ASA version (before you downgrade it). If you cannot achieve compatibility, we suggest you do not perform a downgrade.

### Procedure

**Step 1** At the ASA CLI, copy the backup ASA configuration to the startup configuration. For failover or clustering, perform this step on the active/control unit. This step replicates the command to the standby/data units.

**copy** *old_config_url* **startup-config**

It's important that you do not save the running configuration to the startup configuration using **write memory**; this command will overwrite your backup configuration.

**Example:**

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

**Step 2** In FXOS, use the Firepower Chassis Manager or FXOS CLI to use the old ASA software version using the upgrade procedure in the ASA upgrade guide for standalone, failover, or clustering deployments. In this case, specify the old ASA version instead of a new version.

**Step 3** If you are also downgrading FXOS, use the Firepower Chassis Manager or FXOS CLI to set the old FXOS software version to be the current version using the upgrade procedure in the ASA upgrade guide for standalone, failover, or clustering deployments.

# Downgrade the ASA 5500-X or ISA 3000

The downgrade feature provides a shortcut for completing the following functions on ASA 5500-X and ISA 3000 models:

- Clearing the boot image configuration (**clear configure boot**).
- Setting the boot image to be the old image (**boot system**).
- (Optional) Entering a new activation key (**activation-key**).
- 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.
- Copying the old configuration backup to the startup configuration (**copy** *old_config_url* **startup-config**).
- Reloading (**reload**).

### Before you begin

- This procedure requires a backup configuration of the ASA before you upgraded, so you can restore the old configuration.
- Make sure the ASA FirePOWER module version, if installed, is compatible with the old ASA version. You cannot downgrade the FirePOWER module to an earlier major version.

### Procedure

**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.

**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.

**Step 6** Click **Downgrade**.

# Manage 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.

# Configure File Access

The ASA can use an FTP client, secure copy client, or TFTP client. You can also configure the ASA as a secure copy server so you can use a secure copy client on your computer.

## Configure 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.

### Procedure

**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.

## Configure 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.

### Before you begin

- 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 or wildcards.
- Enable SSH on the ASA according to Configure HTTPS Access for ASDM, Other Clients.
- The ASA license must have the strong encryption (3DES/AES) license to support SSH Version 2 connections.
- Unless otherwise specified, 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.
- The performance of secure copy depends partly on the encryption cipher used. By default, the ASA negotiates one of the following algorithms in order: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. If the first algorithm proposed (3des-cbc) is chosen, then the performance is much slower than a more efficient algorithm such as aes128-cbc. To change the proposed ciphers, use the

**Configuration** > **Device Management** > **Advanced** > **SSH Ciphers** pane; for example, choose **Custom** and set it to aes128-cbc.

### Procedure

**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** Check the **Enable secure copy server** check box.

**Step 3** (Optional) 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, select the server from the Trusted SSH Hosts table, and click **Delete**.

**Step 4** (Optional) 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 5** Click **Apply**.

### Examples

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

**scp -v -pw** *password* [*path*/]*source_filename*
*username@asa_address***:**{**disk0**|**disk1**}**:/**[*path*/]*dest_filename*

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

## Configure 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. In this way, you can back up and propagate configuration files to multiple ASAs.

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

### Procedure

**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**.

## Add Mount Points

You can add a CIFS or FTP mount point.

### Add a CIFS Mount Point

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

### Procedure

**Step 1** Choose **Configuration** > **Device Management** > **Management Access** > **File Access** > **Mount-Points**, and 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**.

### Add an FTP Mount Point

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.

#### Procedure

**Step 1** Choose **Configuration** > **Device Management** > **Management Access** > **File Access** > **Mount-Points**, and 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**.

## Access the File Management Tool

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

**Procedure**

**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 Transfer Files, on page 15 for more information.

**Step 10** Click **Mount Points** to open the Manage Mount Points dialog box. See Add Mount Points , on page 13 for more information.

# Transfer 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.

## Transfer Files Between Local PC and Flash

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

**Procedure**

**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.

## Transfer Files Between Remote Server and Flash

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

**Procedure**

**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.

a) (Optional) Specify the interface through which the ASA communicates with the server. If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table.

b) Choose the path to the location of the file, including the IP address of the server.

**Note** File transfer supports IPv4 and IPv6 addresses.

c) 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.

a) To transfer the file to the flash file system, choose the **Flash file system** option.
b) 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.

a) (Optional) Specify the interface through which the ASA communicates with the server. If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table.
b) Enter the path to the location of the file.
c) 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.

# Set the ASA Image, ASDM, and Startup Configuration

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.

See the following model guidelines:

- Firepower 4100/9300 chassis—ASA upgrades are managed by FXOS; you cannot upgrade the ASA within the ASA operating system, so do not use this procedure for the ASA image. You can upgrade ASA and FXOS separately from each other, and they are listed separately in the FXOS directory listing. The ASA package always includes ASDM.
- Firepower 2100—The ASA, ASDM, and FXOS images are bundled together into a single package. Package updates are managed by FXOS; you cannot upgrade the ASA within the ASA operating system, so do not use this procedure for the ASA image. You *cannot* upgrade ASA and FXOS separately from each other; they are always bundled together.

- ASDM for the Firepower models—ASDM can be upgraded from within the ASA operating system, so you do not need to only use the bundled ASDM image. ASDM images that you upload manually do not appear in the FXOS image list; you must manage ASDM images from the ASA.

  **Note** When you upgrade the ASA bundle, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA because they have the same name (**asdm.bin**). But if you manually chose a different ASDM image that you uploaded (for example, **asdm-782.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should either upgrade ASDM before you upgrade the bundle, or you should reconfigure the ASA to use the bundled ASDM image (**asdm.bin**) just before upgrading the ASA bundle.

- ASAv—The initial deployment ASAv package puts the ASA image in the read-only boot:/ partition. When you upgrade the ASAv, you specify a different image in flash memory. Note that if you later clear your configuration, then the ASAv will revert to loading the original deployment image. The initial deployment ASAv package also includes an ASDM image that it places in flash memory. You can upgrade the ASDM image separately.

See the following default settings:

- ASA image:
  - Physical ASAs—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.
  - Firepower 4100/9300 chassis—The FXOS system determines which ASA image to boot. You cannot use this procedure to set the ASA image.
  - Firepower 2100—The FXOS system determines which ASA/FXOS package to boot. You cannot use this procedure to set the ASA image.
- ASDM image on 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.

### Procedure

**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**.

# Back Up and Restore Configurations or Other Files

We recommend that you make regular backups of your configuration and other system files to guard against system failure.

## Perform a Complete System Backup or Restoration

These procedures describe how to back up and restore configurations and images to a zip file and transfer it to your local computer.

### Before You Begin Backup or Restore

- You should have at least 300 MB of disk space available at the backup or restore location before you start a backup or restore.
- The ASA must be in single context mode.
- If you make any configuration changes during or after a backup, those changes will not be included in the backup. If you change a configuration after making the backup, then perform a restore, this configuration change will be overwritten. As a result, the ASA might behave differently.
- You can start only one backup or restore at a time.
- 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.
- If you use clustering, you can only back up or restore the startup-configuration, running-configuration, and identity certificates. You must create and restore a backup separately for each unit.
- If you use failover, you must create and restore a backup separately for the active and standby units.
- If you set a master passphrase for the ASA, then you 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 Configure the Master Passphrase to learn how to reset it before continuing with the backup.
- 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.

- You cannot back up using the CLI and restore using ASDM, or vice versa.
- Each backup file includes the following content:
  - Running-configuration
  - Startup-configuration
  - All security images

    Cisco Secure Desktop and Host Scan images

    Cisco Secure Desktop and Host Scan settings

    AnyConnect (SVC) client images and profiles

    AnyConnect (SVC) customizations and transforms
  - Identity certificates (includes RSA key pairs tied to identity certificates; excludes standalone keys)
  - VPN pre-shared keys
  - SSL VPN configurations
  - Application Profile Custom Framework (APCF)
  - Bookmarks
  - Customizations
  - Dynamic Access Policy (DAP)
  - Plug-ins
  - Pre-fill scripts for connection profiles
  - Proxy Auto-config
  - Translation table
  - Web content
  - Version information

## Back Up the System

This procedure describes how to perform a complete system backup.

**Procedure**

**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** Only identity certificates are backed up by this process. However, certificate authority certificates are not backed up. For instructions on backing up CA certificates, see Back Up the Local CA Server, on page 24.

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

After clicking OK or Cancel, the backup begins immediately.

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

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

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

## Restore the Backup

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

### Procedure

**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.

The zip file that you restore must be created by choosing the **Tools > Backup Configurations** option.

**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.

# Configure Automatic Backup and Restore (ISA 3000)

On the ISA 3000, you can configure automatic backups to a particular location every time you save your configuration.

Automatic restore lets you easily configure new devices with a complete configuration loaded on an SD flash memory card. Automatic restore is enabled in the default factory configuration.

## Configure Automatic Backup (ISA 3000)

On the ISA 3000, you can configure automatic backups to a particular location every time you save your configuration.

### Before you begin

This feature is only available on the ISA 3000.

### Procedure

**Step 1** Choose **Configuration** > **Device Management** > **Auto Backup & Restore Configuration**.

**Step 2** Check or uncheck **Automate Backup Configuration** to enable or disable automatic backups.

If you enable automatic backups, when you save the configuration, the configuration is automatically saved to the backup location as well as to the startup configuration. The backup file has the name "auto-backup-asa.tgz".

Set the following parameters:

- **Interface**—Specifies the interface to reach the backup URL, if you specify off-device storage. If you do not specify the interface name, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table.
- **Location**—Specifies the storage medium to be used for backing up data. You can specify a URL or local storage. disk0 is the internal flash drive. disk1 is an optional USB memory stick on USB 1. disk2 is an optional USB memory stick on USB 2. And disk3 is the SD memory card. The default for automatic restore is disk3:.
- **Passphrase**—Sets the passphrase to secure the backed-up data. The default for automatic restore is "cisco".

## Configure Automatic Restore (ISA 3000)

Automatic restore mode restores the system configuration on a device without any user intervention. For example, you insert an SD memory card containing a saved backup configuration into a new device and then power the device on. When the device comes up, it checks the SD card to decide if the system configuration needs to be restored. (The restoration is only initiated if the backup file has the "fingerprint" of a different device. The fingerprint of the backup file is updated to match the current device during a backup or restore operation. So if the device has already completed a restore, or if it has created its own backup, then the automatic restore is skipped.) If the fingerprint shows a restoration is required, the device replaces the system configuration (startup-config, running-config, SSL VPN configuration, and so on; see Back Up the System, on page 20 for details about the contents of the backup). When the device finishes booting, it is running the saved configuration.

Automatic restore is enabled in the default factory configuration, so you can easily configure new devices with a complete configuration loaded on an SD memory card without having to perform any pre-configuration of the device.

Because the device needs to decide early in the boot process if the system configuration needs to be restored, it checks ROMMON variables to determine if the device is in automatic restore mode and to obtain the location of the backup configuration. The following ROMMON variables are used:

- **RESTORE_MODE =** {**auto** | **manual**}

  The default is **auto**.

- **RESTORE_LOCATION =** {**disk0:** | **disk1:** | **disk2:** | **disk3:**}

  The default is **disk3:**.

- **RESTORE_PASSPHRASE =** *key*

  The default is **cisco**.

To change the automatic restore settings, complete the following procedure.

### Before you begin

- This feature is only available on the ISA 3000.
- If you use the default restore settings, you need an SD memory card installed (part number SD-IE-1GB=).

- If you need to restore the default configuration to ensure that automatic restore is enabled, use the **configure factory default** command. This command is only available in transparent firewall mode, so if you are in routed firewall mode, use the **firewall transparent** command first.

**Procedure**

**Step 1** Choose **Configuration** > **Device Management** > **Auto Backup & Restore Configuration**.

**Step 2** Check or uncheck **Automate Restore Configuration** to enable or disable automatic restore.

The name of the file that is restored is "auto-backup-asa.tgz". If you enable automatic restore, set the following parameters:

- **Location**—Specifies the storage medium to be used for restoring data. disk0 is the internal flash drive. disk1 is an optional USB memory stick on USB 1. disk2 is an optional USB memory stick on USB 2. And disk3 is the SD memory card. The default is disk3.
- **Passphrase**—Sets the passphrase to read the backed-up data. The default is "cisco".

# Back Up the Local CA Server

When you do an 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.

**Procedure**

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

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

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

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

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

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

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

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

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

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

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

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

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

```
crypto ca server
 no shutdown
```

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

**Step 7** Save the configuration.

# Save the Running Configuration to a TFTP Server

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

**Procedure**

**Step 1** 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.

# Schedule a System Restart

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

**Procedure**

**Step 1** Choose **Tools** > **System Reload**.

**Step 2** In the Reload Scheduling area, define the following settings:

a) For the Configuration State, choose either to save or discard the running configuration at restart time.

b) For the Reload Start Time, choose from the following options:

- Click **Now** to perform an immediate restart.
- Click **Delay by** to delay the restart by a specified amount of time. Enter the time before the restart begins in hours and minutes or only minutes.
- Click **Schedule at** to schedule the restart to occur at a specific time and date. Enter the time of day the restart is to occur, and select the date of the scheduled restart.

c) In the Reload Message field, enter a message to send to open instances of ASDM at restart time.

d) Check the **On reload failure force immediate reload after** check box to show the amount of time elapsed in hours and minutes or only minutes before a restart is attempted again.

e) Click **Schedule Reload** to schedule the restart as configured.

The Reload Status area displays the status of the restart.

**Step 3** Choose one of the following:

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

# Configure 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.

# About Auto Update

This section describes how Auto Update is implemented and why you might want to use Auto Update.

## 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.

# Guidelines for Auto Update

### Context Mode

Auto Update is supported in single context mode only.

### Clustering

No clustering support.

### Models

No support on the following models:

- ASA 5506-X, 5508-X, 5516-X
- Firepower 2100, 4100, and 9300
- ASAv

### Additional Guidelines

- 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.

# Configure Communication with an Auto Update Server

### Procedure

**Step 1** 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.

**Step 2** 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.

**Step 3** 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.

**Step 4** 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.

**Step 5** 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.

**Step 6** 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.

# Monitoring Auto Update

## 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
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.

# History for Software and Configurations

| Feature Name | Platform Releases | Feature Information |
|---|---|---|
| Secure Copy client | 9.1(5)/9.2(1) | The ASA now supports the Secure Copy (SCP) client to transfer files to and from a SCP server.<br>We modified the following screens:<br>Tools > File Management > File Transfer > Between Remote Server and Flash **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server** |
| Configurable SSH encryption and integrity ciphers | 9.1(7)/9.4(3)/9.5(3)/9.6(1) | Users can select cipher modes when doing SSH encryption management and can configure HMAC and encryption for varying key exchange algorithms. You might want to change the ciphers to be more or less strict, depending on your application. Note that the performance of secure copy depends partly on the encryption cipher used. By default, the ASA negotiates one of the following algorithms in order: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. If the first algorithm proposed (3des-cbc) is chosen, then the performance is much slower than a more efficient algorithm such as aes128-cbc. To change the proposed ciphers, use **ssh cipher encryption custom aes128-cbc**, for example.<br>We introduced the following screen: **Configuration** > **Device Management** > **Advanced** > **SSH Ciphers** |
| Auto Update server certificate verification enabled by default | 9.2(1) | 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:<br>`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.`<br>The configuration will be migrated to explicitly configure no verification.<br>We modified the following screen: Configuration > Device Management > System/Image Configuration > Auto Update > Add Auto Update Server. |

| Feature Name | Platform Releases | Feature Information |
|---|---|---|
| System backup and restore using the CLI | 9.3(2) | You can now back up and restore complete system configurations, including images and certificates, using the CLI.<br>We did not modify any ASDM screens. |
| Recovering and loading a new ASA 5506W-X image | 9.4(1) | We now support the recovery and loading of a new ASA 5506W-X image.<br>We did not modify any ASDM screens. |
| Automatic Backup and Restore for the ISA 3000 | 9.7(1) | You can enable auto-backup and/or auto-restore functionality using pre-set parameters in the backup and restore commands. The use cases for these features include initial configuration from external media; device replacement; roll back to an operable state.<br>We introduced the following screen: **Configuration** > **Device Management** > **Auto Backup & Restore Configuration** |