Configuring the Cisco IOS Auto-Upgrade Manager

The Cisco IOS Auto-Upgrade Manager (AUM) feature simplifies the software image upgrade process by providing a simple interface to specify, download, and upgrade a new Cisco IOS image.

You can upgrade to a new Cisco IOS image in interactive mode by allowing the Auto-Upgrade Manager to guide you through the process. Alternatively, you can perform the upgrade by issuing a single Cisco IOS command or a series of commands. All three methods utilize the Warm Upgrade functionality to perform the upgrade and minimize downtime.

- Finding Feature Information, on page 1
- Prerequisites for Cisco IOS Auto-Upgrade Manager, on page 1
- Restrictions for Cisco IOS Auto-Upgrade Manager, on page 2
- Information About Cisco IOS Auto-Upgrade Manager, on page 2
- How to Upgrade a Cisco IOS Software Image Using the Cisco IOS Auto-Upgrade Manager, on page 5
- Configuration Examples for Cisco IOS Auto-Upgrade Manager, on page 9
- Additional References, on page 11
- Feature Information for Cisco IOS Auto-Upgrade Manager, on page 12
- Glossary, on page 12

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Cisco IOS Auto-Upgrade Manager

- You must configure the DNS server IP address on the router for a download from Cisco. For more details, refer to the “Configuring the DNS Server IP Address: Example” section and the “Related Documents” section.

- You must configure the Secure Socket Layer (SSL) certificate from the Cisco website (www.cisco.com) on the router for a download from Cisco. This configuration is not required for a download from a non-Cisco server. For more details, refer to the "Configuring the SSL Certificate for a Cisco Download" section and the "Related Documents" section.
- You must register with Cisco Systems for cryptographic software downloads if you want to download cryptographic Cisco IOS software images.

Restrictions for Cisco IOS Auto-Upgrade Manager

The Cisco IOS Auto-Upgrade Manager will not run to completion if the router does not have sufficient memory resource to load and store the requested Cisco IOS software image. The Cisco IOS software image can be downloaded from www.cisco.com only if the current Cisco IOS software image running in the router is a cryptographic image.

Information About Cisco IOS Auto-Upgrade Manager

Cisco IOS Auto-Upgrade Manager Overview

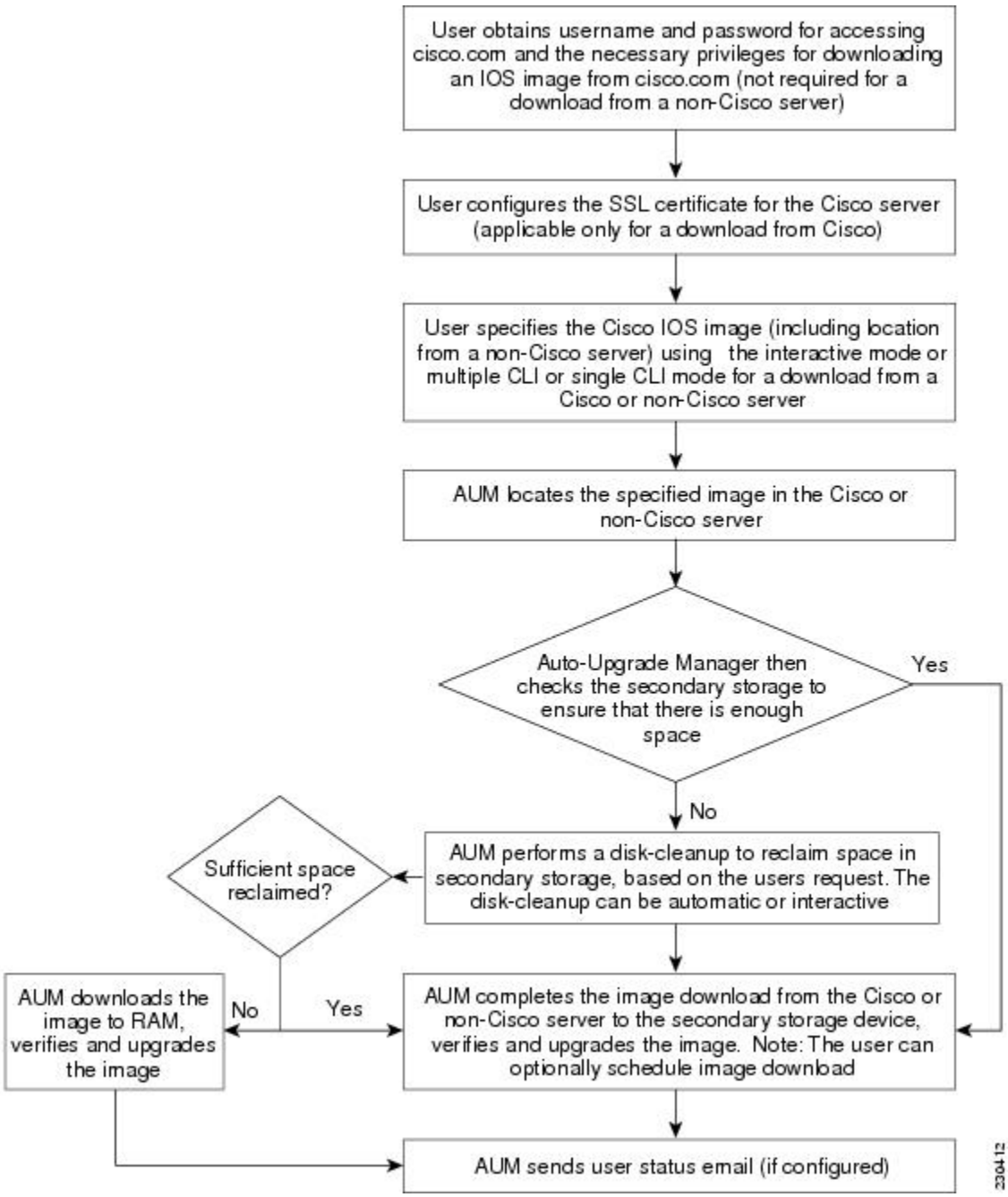
The Cisco IOS Auto-Upgrade Manager streamlines the process of upgrading to a new Cisco IOS software image. You can run the Cisco IOS Auto-Upgrade Manager through the command-line interface (CLI). AUM enables the router to connect to the Cisco website (www.cisco.com) and send the cisco.com username and password for authentication. After authentication, the router passes the name of the Cisco IOS software image that is specified by the user to the Cisco server. The Cisco server returns the complete URL of the Cisco IOS software image to the router.

The Cisco IOS Auto-Upgrade Manager configured on the router can then manage the entire process of upgrading to the Cisco IOS software image. AUM upgrades the router with the software image at the time specified by the user by performing the following tasks:

- Locating and downloading the Cisco IOS software image
- Checking all requirements
- Managing secondary storage space
- Validating the Cisco IOS software image
- Scheduling a warm-upgrade

The figure below illustrates the workflow of the Cisco IOS Auto-Upgrade Manager.

Figure 1: Cisco IOS Auto-Upgrade Manager Workflow



Note If the router fails to load the Cisco IOS software image that you have specified, it displays the error message in the console window and in the syslog buffers indicating the reason for the failure. If the user is not authorized to download encrypted software, an error message is generated requesting the user to register for this service. Similarly, if any CLI configuration statements are not understood by the parser at bootup, it generates an error message and stores the log of the invalid configuration lines in the nvram:invalid-config file. This error message indicates that the Cisco IOS software image that you have specified does not support the same feature set as the old Cisco IOS software image. If the router does not have sufficient secondary storage space to support both the images, but succeeds in the upgrade with the new image, it connects to the Cisco server again and downloads the Cisco IOS software image into a secondary storage. This process erases the existing image.

Specific Cisco IOS Software Image Download from the Cisco Website

You can download a specific Cisco IOS software image from www.cisco.com. AUM uses Secure Socket Layer (SSL) for a secure connection, requiring the user to configure the certificate. The router passes the name of the Cisco IOS software image along with your username and password to log in to the www.cisco.com server. The Cisco server returns the complete URL for the specific Cisco IOS software image to the router.

The Cisco IOS Auto-Upgrade Manager can then automatically download the Cisco IOS software image that you have specified from www.cisco.com, verify it, and upgrade the router with the downloaded image.

Note The Intelligent Download Application (IDA) is the Cisco interface to AUM and is sometimes used interchangeably with the term *Cisco server* in the context of AUM.

Additionally, the Cisco IOS Auto-Upgrade Manager provides the following optional services:

- Disk clean-up utility
- Scheduling of upgrade

These services are available for download from a Cisco or non-Cisco server, both in the interactive and command line modes.

Specific Cisco IOS Software Image Download from a Non-Cisco Server

You can download a Cisco IOS software image that is present on a local or non-Cisco TFTP or FTP server. You can provide an FTP username and password using the **ipftpusername** and **ipftppassword**global configuration commands for an FTP download. The Cisco IOS Auto-Upgrade Manager automates the process of downloading the specific Cisco IOS software image from a non-Cisco server and warm upgrade services. It also provides the disk clean-up utility to delete the files if the space required to download the new Cisco IOS software image is not sufficient.

Interactive and Single Command Line Mode

You can download a specific Cisco IOS software image from www.cisco.com using the CLI or through the following user interfaces:

Interactive Mode

The Auto-Upgrade Manager guides you through the process of upgrading to a new Cisco IOS image in the interactive mode. When you choose automatic upgrade, you are required to answer a few questions in the interactive mode to complete the device upgrade. You can initiate interactive mode by issuing the **upgradeautomatic** command without any options. For more details, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

Single Command Line Mode

The non-interactive single line CLI is for advanced users. You can download and upgrade to a new Cisco IOS software image from a Cisco or non-Cisco server by using the **upgradeautomaticgetversion** command and specifying all the required arguments. For more details, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

The interactive mode and single line CLI mode are applicable to downloads from Cisco and non-Cisco servers.

How to Upgrade a Cisco IOS Software Image Using the Cisco IOS Auto-Upgrade Manager

Configuring the SSL Certificate for a Cisco Download

Perform this task to configure the SSL certificate for a Cisco download.

Before you begin

The SSL certificate must be configured to download from cisco.com. The certificate is required for secure HTTP communication. You can obtain the SSL certificate from the Cisco website (www.cisco.com) to configure it on the router.

Perform the following task to obtain the SSL certificate from the Cisco website:

1. Pull down the Tools menu in Internet Explorer (IE) and select Internet Options.
2. Under the Advanced tab, select “Warn if changing between secure and not secure mode.”
3. Enter the URL https://www.cisco.com in IE. When a security alert pop-up box appears, click “No” for the question “You are about to leave a secure Internet connection. Do you want to continue?”.
4. Double-click the lock icon on the status bar of IE. This action opens a dialog box showing the details of the certificate.
5. Click the Certification Path tab. This tab displays the certification chain.
6. Select each CA certificate and click View Certificate. This action opens a details window for the certificate.
7. Select the Details tab of the certificate window displayed, and click Copy to File. This action opens the certificate export wizard.
8. Save the certificate in the Base-64 encoded format to a file (such as cisco.cert).
9. Open the cisco.cert file in a Notepad to get the certificate data that you need to configure on your router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment terminal**
5. **revocation-check none**
6. **exit**
7. **crypto ca authenticate** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki trustpoint** *name* **Example:** `Device(config)# crypto pki trustpoint cisco_ssl_cert`	Declares the certification authority (CA) and enters ca-trustpoint configuration mode.
Step 4	**enrollment terminal** **Example:** `Device(ca-trustpoint)# enrollment terminal`	Displays the certificate request on the console terminal and allows you to enter the issued certificate data on the terminal.
Step 5	**revocation-check none** **Example:** `Device(ca-trustpoint)# revocation-check none`	Specifies that certificate checking is not required.
Step 6	**exit** **Example:** `Device(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 7	**crypto ca authenticate** *name* **Example:** `Device(config)# crypto ca authenticate cisco_ssl_cert`	Authenticates the CA to your router by obtaining the self-signed certificate of the CA.

Configuring the Cisco IOS Auto-Upgrade Manager

Perform this task to configure the Cisco IOS Auto-Upgrade Manager.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **autoupgrade disk-cleanup** {**crashinfo** | **core** | **image** | **irrecoverable**}
4. **autoupgrade ida url** *url*
5. **autoupgrade status email** {**recipient***email-address* | **smtp-server***name-address*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**autoupgrade disk-cleanup** {**crashinfo** | **core** | **image** | **irrecoverable**} **Example:** `Device(config)# autoupgrade disk-cleanup crashinfo`	Configures the Cisco IOS Auto-Upgrade Manager disk cleanup utility.
Step 4	**autoupgrade ida url** *url* **Example:** `Device(config)# autoupgrade ida url https://www.cisco.com/cgi-bin/new-ida/locator/locator.pl`	Configures the URL of the Cisco server running on www.cisco.com where the image download requests will be sent by Cisco IOS Auto-Upgrade Manager. **Note** This step is required only if the default URL has changed.
Step 5	**autoupgrade status email** {**recipient***email-address* | **smtp-server***name-address*} **Example:** `Device(config)# autoupgrade status email smtp-server smtpserver.abc.com`	Configures the email address and outgoing email server to which the router sends the status email.

Downloading the Cisco IOS Software Image

Perform this task to download the Cisco IOS software image from the Cisco website (www.cisco.com) or from a non-Cisco server.

SUMMARY STEPS

1. **enable**
2. **upgrade automatic getversion** {**ciscousername***username***password***password***image***image* | *url*} [**at***hh*:*mm* | **now** | **in***hh*:*mm*] [**disk-management** {**auto** | **confirm** | **no**}]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**upgrade automatic getversion** {**ciscousername***username***password***password***image***image*	*url*} [**at***hh*:*mm*	**now**	**in***hh*:*mm*] [**disk-management** {**auto**	**confirm**	**no**}] **Example:** `Device# upgrade automatic getversion tftp://abc/tom/c3825-adventerprisek9-mz.124-2.XA.bin at now disk-management auto`	Downloads the image directly from www.cisco.com or a non-Cisco server.

Reloading the Router with the New Cisco IOS software Image

Perform this task to reload the router with the new Cisco IOS software image.

SUMMARY STEPS

1. **enable**
2. **upgrade automatic runversion** [**at***hh*:*mm* | **now** | **in***hh*:*mm*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**upgrade automatic runversion** [**at***hh*:*mm*	**now**	**in***hh*:*mm*]	Reloads the router with the new image.

	Command or Action	Purpose
	Example: `Device# upgrade automatic runversion at 7:30`	**Note** You can also use the **upgradeautomaticgetversion** command to reload the router with the new Cisco IOS software image. But, if you have already downloaded the Cisco IOS software image using the **upgradeautomaticgetversion** command, you must use the **upgradeautomaticrunversion** command to reload the router.

Canceling the Cisco IOS Software Image Reload

Perform this task to cancel a scheduled reload of a specific Cisco IOS software image.

You can cancel an image reload under the following conditions:

- When the scheduled time to reload the router is not sufficient.
- When you do not want to upgrade the router to the new image.

SUMMARY STEPS

1. **enable**
2. **upgrade automatic abortversion**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**upgrade automatic abortversion** **Example:** `Device# upgrade automatic abortversion`	Cancels the Cisco IOS software image upgrade.

Configuration Examples for Cisco IOS Auto-Upgrade Manager

Configuring the DNS Server IP Address Example

You should configure the DNS server IP address on the router before configuring the Cisco IOS Auto-Upgrade Manager. This sequence of events enables the router to use the **ping** command with a hostname rather than an IP address. You can successfully ping the Cisco website (www.cisco.com) after configuring the DNS server IP address on the router. This action also ensures that the router is connected to the Internet.

The following example shows how to configure the DNS server IP address on your router. After configuring the DNS server IP address, you should be able to ping www.cisco.com successfully.

```
configure terminal
 ip domain name mycompany.com
 ip name-server 10.2.203.1
 end
  ping www.cisco.com
```

Configuring the SSL Certificate for a Cisco Download Example

You should configure the SSL certificate of the Cisco server on the router before using the Cisco IOS Auto-Upgrade Manager to download an image from the Cisco website.

The following example shows how to configure the SSL certificate:

```
configure terminal
 crypto pki trustpoint cisco_ssl_cert
  enrollment terminal
  revocation-check none
  exit
 crypto ca authenticate cisco_ssl_cert
!Enter the base 64 encoded CA certificate and end this with a blank line or the word quit
. !The console waits for the user input. Paste the SSL certificate text and press Return.

-----BEGIN CERTIFICATE-----


<The content of the certificate>

-----END CERTIFICATE-----


!Trustpoint 'cisco_ssl_cert' is a subordinate CA and holds a non self signed cert
!Trustpoint 'cisco_ssl_cert' is a subordinate CA.
!but certificate is not a CA certificate.
!Manual verification required
!Certificate has the following attributes:
      ! Fingerprint MD5: 49CE9018 C0CC41BA 1D2FBEA7 AD3011EF
      ! Fingerprint SHA1: A88EAA5D 73D63CB7 BF25197B 9C35ED97 023BB57B

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

Configuring the Cisco IOS Auto-Upgrade Manager Example

The following example shows how to configure the Cisco IOS Auto-Upgrade Manager on the router:

```
configure terminal
autoupgrade disk-cleanup crashinfo
autoupgrade ida url https://www.cisco.com/cgi-bin/new-ida/locator/locator.pl
autoupgrade status status email smtp-server
```

Additional References

The following sections provide references related to the Cisco IOS Auto-Upgrade Manager.

Related Documents

Related Topic	Document Title
Cisco IOS Auto-Upgrade Manager commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	Cisco IOS Configuration Fundamentals Command Reference
Configuring DNS on Cisco routers	Configuring DNS on Cisco Routers technical note
Warm Upgrade	Warm Upgrade feature module

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Cisco IOS Auto-Upgrade Manager

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Cisco IOS Auto-Upgrade Manager

Feature Name	Releases	Feature Information
Cisco IOS Auto-Upgrade Manager	12.4(15)T Cisco IOS XE Release 3.9S	The Cisco IOS Auto-Upgrade Manager simplifies the software image upgrade process by providing a simple interface to specify, download, and upgrade a new Cisco IOS image. In 12.4(15)T, this feature was introduced on the Cisco 1800, Cisco 2800, and Cisco 3800 series routers. This feature was integrated into Cisco IOS XE Release 3.9S. The following commands were introduced or modified by this feature: **autoupgrade disk-cleanup**,**autoupgrade ida url**, **autoupgrade status email**, **debug autoupgrade**, **show autoupgrade configuration unknown**, **upgrade automatic abortversion**, **upgrade automatic getversion**, **upgrade automatic runversion**.

Glossary

CLI --command-line interface

IDA or Cisco server --Intelligent Download Application

Cisco IOS --Cisco Internetworking Operating System