

Cisco IOS Auto-Upgrade Manager

Cisco IOS® Auto-Upgrade Manager automates the process of upgrading Cisco IOS Software versions on Cisco® 1800, 2800, and 3800 Series Integrated Services Routers directly from the console without additional management software. Whether for a single device or multiple devices, Cisco IOS Auto-Upgrade Manager guides the user through the process of downloading the software to the router and scheduling the upgrade with easy-to-use, interactive mode prompts. More advanced users can take advantage of the Cisco IOS Auto-Upgrade Manager “single-line” command to initiate the process. Either way, Cisco IOS Auto-Upgrade Manager can help reduce the cost of upgrading systems by streamlining the process to perform Cisco IOS Software upgrades by engineers of varying skill levels.

Product Overview

Cisco IOS Auto-Upgrade Manager manages and simplifies the process of upgrading (or downgrading) Cisco IOS Software versions on Cisco 1800, 2800, and 3800 Series Integrated Services Routers. The user interface to Cisco IOS Auto-Upgrade Manager, which is through the console, can be a series of easy-to-use, conversational mode prompts; a single-line command; or several nonprompted commands, depending on the user's familiarity with upgrading software versions. Cisco IOS Auto-Upgrade Manager loads the new software version from Cisco or any FTP or Trivial File Transport Protocol (TFTP) server the user specifies. The application checks to ensure that the router has enough free memory on secondary storage for the software image, and if not, cleans up secondary storage to free space for the image. After validating the image, it schedules the upgrade, incorporating capabilities introduced with Warm Upgrade to minimize downtime and provide automatic rollback if the new version fails to initialize. Cisco IOS Auto-Upgrade Manager can send a status e-mail on completion, and the application keeps a file of any old configuration lines that are no longer valid.

The Challenge

Users upgrade Cisco IOS Software periodically for a variety of reasons: They may need new features or functions to implement new services, they may wish to standardize software versions in their company network to ease support, or they may find a security vulnerability or software bug that can be eliminated with a later version of Cisco IOS Software. Whatever the reason for the upgrade, when the new version is identified, the network engineer must find the software version, download it to a server, transfer it to the router or switch, and then schedule the upgrade and manually reload the device. Cisco provides management software that can help with that process, such as CiscoWorks, but that software may not always be available to the person performing the upgrade. Although upgrading Cisco IOS Software manually is not difficult, users unfamiliar with the process may still be intimidated. More experienced users may find the process cumbersome - especially if they have a large number of systems to upgrade.

The Solution: Cisco IOS Auto-Upgrade Manager

Cisco IOS Auto-Upgrade Manager simplifies upgrading Cisco IOS Software versions on Cisco 1800, 2800, and 3800 Series Integrated Services Routers for both novices and experienced network engineers. When in enable mode, novice users need only to issue a simple command, upgrade automatic to begin an interactive script that guides them through the process of downloading the new software and performing the upgrade. More experienced users can avoid the detailed script and issue either a series of commands to step through the process or a single command with all the required information to quickly load the new software and perform the upgrade (refer to the

example in Figure 1). All these methods accomplish the same thing. The single-line method can be quite useful when upgrading multiple systems, especially if they are being upgraded to the same software version.

Figure 1. Single-Line Command

```
Router # upgrade automatic getversion {cisco username username password pass image  
image / url } [at hh:mm | now | in hh:mm] [disk-management auto | confirm | no]
```

How It Works

Cisco IOS Auto-Upgrade Manager performs several tasks. First, it finds the specified software and loads it on the system to be upgraded. The user must provide the image name and location. The image name can be obtained from any of numerous sources, including research the user has done, often on the Cisco Software Center (<http://www.cisco.com/cisco/web/download/index.html>); a recommendation from a Cisco engineer, an authorized Cisco partner organization, the Cisco Technical Assistance Center, or other source. Cisco IOS Auto-Upgrade Manager can obtain the software version from Cisco (the default) or other FTP or TFTP server that may be on the user's internal network or even possibly a partner site. When downloading from Cisco, the Cisco IOS Auto-Upgrade Manager uses Secure Sockets Layer (SSL) for a secure connection, requiring the user to configure the Cisco SSL certificate (refer to the Cisco IOS Auto-Upgrade Manager feature documentation for details). Cisco IOS Auto-Upgrade Manager then checks to ensure that there is enough space in secondary storage (usually flash memory) to store the image. If not, it attempts to make enough space by performing a disk clean-up. If the application cannot find or make space, it attempts to upgrade the router directly with the source image, and then deletes the previous image and downloads the new image to secondary storage. It terminates the process if direct upgrade is not possible or if it is not accepted by the user. Otherwise, it downloads the new software version onto secondary storage and, if downloading from Cisco, verifies the image. It sends the console status messages of the progress and ultimate success or failure of the download.

Next Cisco IOS Auto-Upgrade Manager must perform the actual upgrade of the system software at the time the user specified. The auto-upgrade manager uses the existing Warm Upgrade capability to perform this upgrade, so the new version is decompressed and loaded into RAM before the system reloads. This process can significantly reduce the system downtime. If the Warm Upgrade process fails, the system "rolls back" to the old software version. During a successful Warm Upgrade, the application keeps a record of any configuration lines that the new software version does not understand, a situation that can happen if a command has been changed or eliminated in newer software, but is more common when downgrading to older software that may not support all of the configured functions. The application stores this record in the file system, and users can view it by using the `show autoupgrade configuration unknown` command.

Finally, Cisco IOS Auto-Upgrade Manager logs the status of the upgrade and, if configured, sends the user a status e-mail. Many e-mail systems can also generate a page with the status information.

Applications

Cisco IOS Auto-Upgrade Manager can be used in many environments. As mentioned previously, the interactive mode of Cisco IOS Auto-Upgrade is quite useful for novice users, guiding them through each step of the upgrade process. Similarly, this mode can also be helpful when providing telephone support to novice users. The single-line mode streamlines the upgrade process for experienced users. The single command line can easily be scripted or entered through a "copy and paste" operation, simplifying the repetitive process of upgrading multiple systems at the same time. Users can schedule the Warm Reload at a convenient time, immediately or delayed, helping minimize the effect of the short outage associated with upgrades.

Prerequisites

Cisco IOS Auto-Upgrade Manager involves three basic requirements. Loading Cisco IOS Software to a system requires that the system have enough free memory (or the ability to free enough memory) to store the Cisco IOS Software image, network connectivity to the server on which that software resides, and authorization to download from that server. Cisco IOS Auto-Upgrade Manager can load software from any FTP or TFTP server to which the system being upgraded has access. The user must ensure that connectivity exists, that the transfer is not blocked by a firewall or other filter, and that appropriate user access is available (usually “anonymous”). Security requirements to download Cisco IOS Software follow:

- The feature set must be Cisco IOS Advanced Security or higher (for HTTPS support).
- The system being upgraded must have Internet connectivity that allows HTTPS (not blocked by a firewall).
- The user must have a registered username and password on Cisco.com and have completed the Encryption Entitlement Form. Users are automatically prompted for this information the first time they select a strong cryptographic image for download directly in the Cisco Software Center; the form is also available at: <http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y>.
- The SSL certificate for the Cisco IOS Auto-Upgrade Manager must be configured (refer to documentation for instructions).

Feature Availability

Cisco IOS Auto-Upgrade Manager is available on Cisco 1800, 2800, and 3800 Series Integrated Services Routers with Cisco IOS Software Release 12.4(15)T and later.

To Download the Software

Visit the [Cisco Software Center](#) to download Cisco IOS Software.

For More Information

For more information about the Cisco IOS Auto-Upgrade Manager, contact your local Cisco account representative.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (10020)